A Trading Model and Security Regime for Mobile e-Commerce via Ad Hoc Wireless Networking

Husna Osman

Submitted for the degree of Doctor of Philosophy

Heriot-Watt University

School of Mathematical and Computer Sciences

August 2016

Abstract

Ad hoc wireless networking offers mobile computer users the prospect of trading with others in their vicinity anywhere anytime. This thesis explores the potential for developing such trading applications. A notable difficulty in designing their security services is being unable to use trusted parties. No one can be guaranteed present in each ad hoc wireless network session. A side benefit is that their costs don't have to be paid for.

A reference model is defined for ad hoc m-commerce and a threat model is formulated of its security vulnerabilities. They are used to elicit security objectives and requirements for such trading systems. Possible countermeasures to address the threats are critically analysed and used to design security services to mitigate them. They include a self-organised P2P identity support scheme using PGP certificates; a distributed reputation system backed by sanctions; a group membership service based on membership vouchers, quorate decisions by some group members and partial membership lists; and a security warning scheme.

Security analysis of the schemes shows that they can mitigate the threats to an adequate degree to meet the trading system's security objectives and requirements if users take due care when trading within it. Formal verification of the system shows that it satisfies certain safety properties.

Acknowledgements

Firstly, I would like to express my gratitude to my primary supervisor **Dr. Hamish Taylor** for his dedication, support, invaluable advice and patience during my time at Heriot-Watt University and throughout the writing of this thesis. Not forgotten to my second supervisor **Dr. Peter JB King** for his continuous support for my PhD work. Without their persistent help, this work would not have been possible to complete.

I would also like to thank my whole family, especially my parents Osman Awang Puteh and Mariah Hassan, my husband Syed Hisham Alwi Syed Ibrahim and my two children Syed Amir Haikal Syed Hisham Alwi and Sharifah Alyaa Haziqah Syed Hisham Alwi, who have always been with me and encouraging me from the very beginning of my PhD life, and whose love have helped me reach this far.

Finally, I am also grateful to my fellow friends and many others whose names are not been mentioned for their encouragement, support and concern throughout the completion of this PhD work.

ACADEMIC REGISTRY
Research Thesis Submission

Name*:*	HUSNA OSMAN		
School/PGI:	SCHOOL OF MATHEMATICAL AND COMPUTER SCIENCES		
Version: *(i.e. First, Resubmission, Final)*	FINAL	Degree Sought (Award **and** Subject area)	DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

Declaration

In accordance with the appropriate regulations I hereby submit my thesis and I declare that:

1) the thesis embodies the results of my own work and has been composed by myself
2) where appropriate, I have made acknowledgement of the work of others and have made reference to work carried out in collaboration with other persons
3) the thesis is the correct version of the thesis for submission and is the same version as any electronic versions submitted*.
4) my thesis for the award referred to, deposited in the Heriot-Watt University Library, should be made available for loan or photocopying and be available via the Institutional Repository, subject to such conditions as the Librarian may require
5) I understand that as a student of the University I am required to abide by the Regulations of the University and to conform to its discipline.

* *Please note that it is the responsibility of the candidate to ensure that the correct version of the thesis is submitted.*

Signature of Candidate*:*		Date:	02/08/2016

Submission

Submitted By *(name in capitals):*	
Signature of Individual Submitting:	
Date Submitted:	

For Completion in the Student Service Centre (SSC)

Received in the SSC by *(name in capitals):*			
Method of Submission *(Handed in to SSC; posted through internal/external mail):*			
*E-thesis Submitted (**mandatory for final theses)***			
Signature:		Date:	

Please note this form should bound into the submitted thesis.

Updated February 2008, November 2008, February 2009, January 2011

Declaration

I declare that this PhD thesis was authored by myself and the work contained herein is my own, unless explicitly stated otherwise. The following articles were published during my research.

- Husna Osman and Hamish Taylor, "Towards a reference model for m-commerce over ad hoc wireless networks," Proceedings of E-Activity and Leading Technologies Conference, 2008, IASK, pp. 223-232.
- Husna Osman and Hamish Taylor, "Managing group membership in ad hoc m-commerce trading systems," Proceedings of 10th Annual International Conference on New Technologies of Distributed Systems, 2010, IEEE, pp. 173-180.
- Husna Osman and Hamish Taylor, "Identity support in a security and trust service for ad hoc m-commerce trading systems," Proceedings of 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications. 2011, IEEE, pp. 285-290.

Contents

List of Figures

List of Tables

Glossary

AP Access Point.

ATM Automated Teller Machine.

B2B Business-to-Business.

B2C Business-to-Consumer.

BAN Body Area Network.

BPMN Business Process Modeling Notation.

CA Certification Authority.

DoD Department of Defense.

DTN Delay Tolerant Networking.

EDGE Enhanced Data rates for Global Evolution.

EFTPOS Electronic Funds Transfer at Point of Sale.

GPRS General Packet Radio Service.

GPS Global Positioning System.

GSM Global System for Mobile Communications.

HSPA High Speed Packet Access.

IoT Internet of Things.

IP Intellectual Property.

JTNC Joint Tactical Networking Center.

JTRS Joint Tactical Radio System.

LTL Linear Temporal Logic.

MAN Metropolitan Area Network.

MANET Mobile Ad Hoc Network.

P2P Peer-to-Peer.

PAN Personal Area Network.

PGP Pretty Good Privacy.

PKI Public Key Infrastructure.

POS Point of Sales.

PROMELA Process Meta-Language.

RCA Root Certification Authority.

RFID Radio Frequency Identification.

SPIN Simple Promela Interpreter.

TTL Time-to-Live.

UMTS Universal Mobile Telecommunications System.

VP Virtual Partitioning.

WLAN Wireless LAN.

WNW Wideband Networking Waveform.

Chapter 1

Introduction

1.1 Context

Ad hoc wireless networking is a promising technology for future wireless communication applications that offers flexible, convenient to set up and inexpensive deployment. It has already been in use since the 1970s, mainly for military operations [173],[41],[107]. One example of the military systems that utilizes ad hoc wireless networks is the Joint Tactical Radio System (JTRS) [55],[52],[33],[149],[130] that was created by the US Department of Defense (DoD) to provide a networked battlefield communications for warfighters to exchange data, voice and video across the battlefield domains. However, due to the restructuring of its program that was responsible for the development of Wideband Networking Waveform (WNW) in 2012, JTRS is now called as the Joint Tactical Networking Center (JTNC) [19]. WNW is a key component of JTRS that was developed to provide advanced wireless communication waveform for land combat operations, which include communications between dismounted soldiers, unmanned vehicles, sensors and so on.

In the past few years, with the advancement of mobile devices and rapid improvement in wireless communication technologies [103], there has been significant progress in research and development in ad hoc wireless networks [122],[131],[97],[73], including in areas outside military operations. With this development, it is likely that ad hoc wireless networks will become more widely used in the near future, especially in its present application domains such as battlefield areas, emergency and rescue operations and with sensor networks. Also, there is a potential for ad hoc wireless networks to be used for commercial purposes, such as to facilitate new business opportunities for users with profitable commercial enterprises, enabling ad hoc wireless network applications to move from military or emergency uses to commercial ones. Although ad hoc wireless networks offer similar advantages for both

military operations and commercial activities, such as quick and inexpensive deployment, no central point of control, self-configuring and so on, their implementation has several fundamental differences which include the following:

Purpose of deployment - In military operations, ad hoc wireless networks are used to establish a quick and reliable communication between soldiers, vehicles and other military equipment in order to relay situational awareness information among a group of soldiers, coordinate military objects, shutdown hostile devices and etc. In contrast, in commercial or business activities, ad hoc wireless networks are used as an alternative solution to enable a group of users or traders who are in the vicinity of each other to exchange information and collaborate with each other to accomplish a specific task or to carry out online trading.

Environment - In battlefield operations, ad hoc wireless networks may be deployed in inhospitable terrains or hostile environments. On the other hand, in commercial activities, ad hoc wireless networks are usually used in normal environments or when the need for such activities arises.

Security - Another difference is that military operations require stricter security requirements compared to the commercial activities due to the high mobility of the network and harsh environment of the battlefield.

Table 1.1 below summarizes the fundamental differences between the utilization of ad hoc wireless networks in military operations and commercial activities:

	Military Operations	**Commercial Activities**
Purpose of Deployment	Communication between soldiers, vehicles and other military equipment to relay situational awareness information, coordinate military objects, shutdown hostile devices and etc	Communication between a group of users or traders to exchange information and collaborate with each other to accomplish a specific task or to carry out online trading
Environment	Hostile Environment	Normal Environment
Security	Stricter security requirements compared to commercial activities	Adequate Security

Table 1.1: Fundamental differences between the utilization of ad hoc wireless networks in military operations and commercial activities

Although there has been a growing interest in utilizing ad hoc wireless networks for commercial or business activities in the recent years [71],[73], there is still little effort geared towards exploring or investigating the viability of its implementation in the real world. Thus, to facilitate research in the commercial area for ad hoc

wireless networks, this thesis introduces a new concept termed ad hoc m-commerce, where an ad hoc wireless network is used as the communication medium for traders to carry out m-commerce transactions. Current implementations of m-commerce only utilise network infrastructures provided by a network service provider.

This thesis uses the term "ad hoc m-commerce trading system" to refer to a type of local trading facility that is conducted online and wirelessly outside infrastructure supported computer networks [117]. It offers interesting opportunities for more convenient and cost effective m-commerce transactions. It enables traders who are equipped with mobile devices, suitable networking capability and appropriate software applications to spontaneously organize themselves into a trading system [118] and then engage in online trading when the need arises regardless of time or location and without relying on any infrastructure support from a network service provider. Members of a trading system will utilize their available computing resources and also their neighbours to communicate and collaborate with each other in m-commerce transactions and other activities of the trading system. However, the nature of an ad hoc wireless network such as its lack of network infrastructures, having a dynamic network topology, using resource constrained mobile devices and so on, means that performing m-commerce transactions over ad hoc wireless networks introduces additional challenges as compared to infrastructure-supported m-commerce.

One of these issues that requires careful consideration when deploying an ad hoc m-commerce trading system in the real-world is how it handles security which impacts on whether users feel confident to use it. This is because this type of trading system's activities and communications among its members are carried out over interceptible radio communication in an ad hoc wireless network and no network service provider can be relied upon to be present to provide security services to its participating parties. If the trading system lacks security mechanisms, it may not only degrade users' confidence to participate in its transactions, but its usage and development will also be inhibited. Thus, it is important for this kind of trading system to have security services that safeguard its operations to a sufficient degree for traders to be prepared to engage in its transactions or activities. However, due to the nature of an ad hoc wireless network and the characteristics of ad hoc m-commerce, the design of security services for an ad hoc m-commerce trading system is challenging and complex. Most of the security schemes for wired networks, computationally intensive processing and power hungry operating arrangements such as the conventional Public Key Infrastructure (PKI) seem unlikely to work well or to be feasible for an ad hoc m-commerce trading system due to the infrastructure-less nature and dynamic network topology of ad hoc wireless networks, as well as the mobile devices' energy constraints [11],[129],[113].

1.2 Research Scope and Objectives

The scope of this research is to present a reference model for an ad hoc m-commerce that articulates clearly the nature and requirements for performing wireless trading outside infrastructure supported computer networks, as well as laying out the key issues involved in performing such trading. The model establishes a taxonomy of terminologies and definitions for describing the ad hoc m-commerce concept, identifies all the functional elements in an ad hoc m-commerce trading system and clarifies dependencies among them. The model also identifies the issues that need to be addressed in order to realise such a system practically. With regard to this reference model, this research is concerned with the security issues in particular, rather than issues such as mobile device limitations, wireless network bandwidth, connectivity, transaction management and etc. A threat model is defined to identify potential threats and vulnerabilities that could subvert the functionality of the trading system, as well as helping to elicit the key security requirements for a security and trust service. The identified threats are classified into three main categories, namely identity-related threats, information-related threats and misbehaviour-related threats. A novel conceptual framework, a trading model and an abstract architecture of an ad hoc m-commerce trading system are also proposed and used as a basis for designing security schemes for a security and trust service in an ad hoc m-commerce trading system to address the identified threats. Figure 1.1 (page 5) illustrates the scope of the research.

The objectives that guide the research are to:

I. Study, analyse and explore the potential of an ad hoc wireless network to be utilized as an alternative way to facilitate m-commerce transactions.

II. Identify and classify potential threats and vulnerabilities that could subvert the functionality of an ad hoc m-commerce trading system.

III. Identify key security requirements for the design of a security and trust service for an ad hoc m-commerce trading system.

IV. Study, analyse and classify possible countermeasures that can be used to address or at least mitigate the identified threats and vulnerabilities, and suit the nature, characteristics and security requirements of an ad hoc m-commerce trading system.

V. Present a general framework for an ad hoc m-commerce trading system that provides a foundation for application developers to organize the effective development, maintenance and enhancement of such trading systems, and serves as

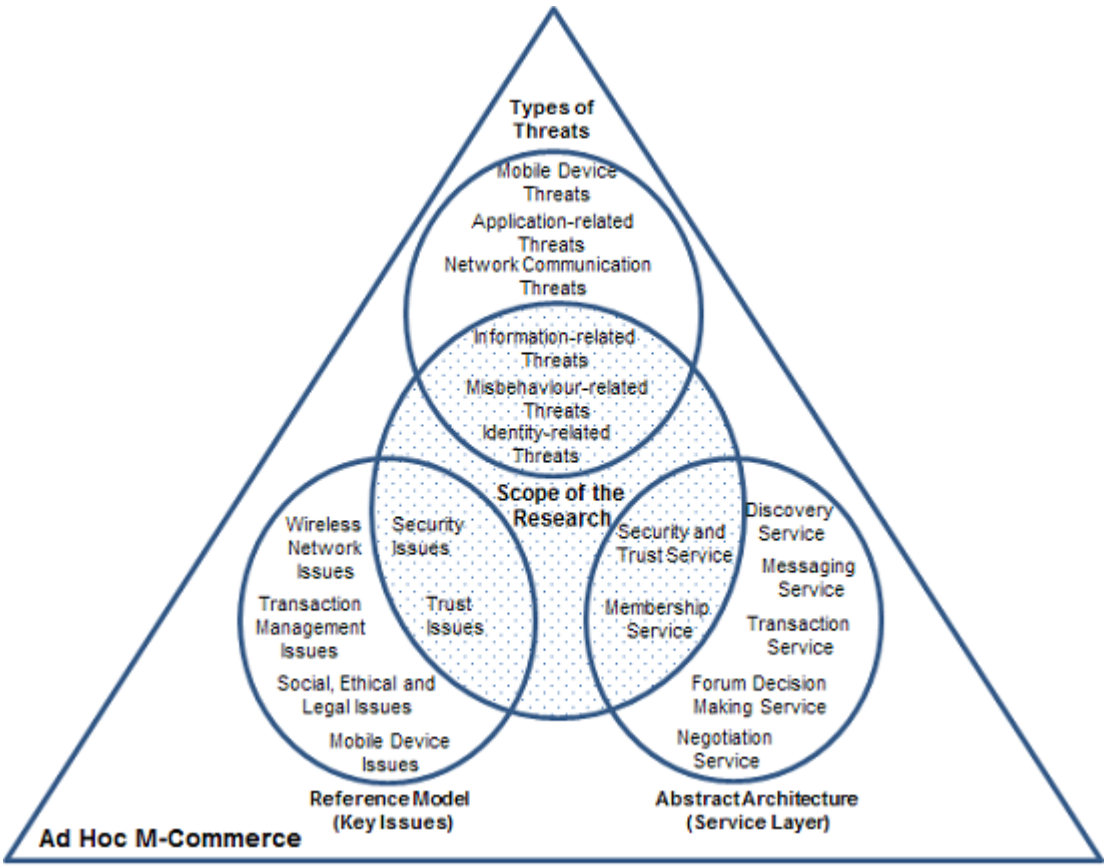


Figure 1.1: Scope of the research

a basis for addressing the major security issues involved in ad hoc m-commerce transactions.

VI. Design and analyse the security schemes in a security and trust service in an ad hoc m-commerce trading system that addresses the identified threats and vulnerabilities to an acceptable level.

VII. Verify that the processes of an ad hoc m-commerce trading system satisfy certain safety properties.

1.3 Research Methodology and Approach

This research has been conducted using the following methodologies:

1. Information Gathering and Analysis

At an early stage of this research work, literature searches were carried out to develop a thorough understanding of the background and complex issues at stake in the area of ad hoc wireless networks and m-commerce. In this process, the nature of an ad hoc wireless network, and the characteristics, main entities and key functional

components of current implementations of m-commerce that utilize infrastructure-based architectures were analysed, and their general requirements and issues were outlined. The main entities, key components and target applications of ad hoc m-commerce, as well as the potential and challenges of its implementation were identified. The outcome of this phase is the ad hoc m-commerce reference model.

2. Threat Modeling

A threat model was developed to help formulate security objectives for ad hoc m-commerce trading systems, and identify possible threats and vulnerabilities that could subvert the functionality of such a trading system. Based on the threat model, the key security requirements for an ad hoc m-commerce trading system and possible countermeasures to address or mitigate the identified threats and vulnerabilities were identified.

3. Framework Formulation

An important part in this research was the formulation of a general framework for an ad hoc m-commerce trading system that provides a novel paradigm for pure Peer-to-Peer (P2P) m-commerce. It includes a trading model for such dealings, and core services that are required to support its functionality and security.

4. Security Architecture Design

A security scheme for a trust and security service in an ad hoc m-commerce trading system was designed to provide security. The security scheme includes an identity support scheme, a fully distributed reputation system and a group membership service.

5. Security Analysis

A security analysis was carried out to evaluate the effectiveness of the proposed design of a security and trust service for an ad hoc m-commerce trading system to address or mitigate the vulnerabilities identified in the threat model. Security was evaluated by critical analysis, where the means by which the proposed security schemes might be compromised by ill-intentioned parties were highlighted and the measures to address their threats were critically analysed and reviewed.

6. Formal Verification

A formal verification of an ad hoc m-commerce trading system was conducted using the SPIN model checker to verify certain safety properties.

1.4 Contributions to Knowledge

The following are the principal contributions to knowledge made by this thesis.

1) The novel ad hoc m-commerce reference model [117] establishes a taxonomy of terminologies, concepts and definitions required for describing ad hoc m-commerce, and identifies all the functional elements in ad hoc m-commerce systems. The model also identifies issues that might restrain the development of such systems. It is intended to allow future researchers to grasp the key issues involved in trading wirelessly among computing nodes in the absence of a network service provider. This reference model should also be useful in identifying and facilitating Research and Development (R&D) for a wide range of ad hoc m-commerce applications. (Chapter 2)

2) The novel threat model specifies the security objectives and key assets of an ad hoc m-commerce trading system. The model also identifies and classifies the possible threats and vulnerabilities that could subvert the functionality of such a trading system. The identified threats are classified into three main categories, namely identity-related threats, information-related threats and misbehaviour-related threats. (Chapter 3)

3) Key security requirements are identified for an ad hoc m-commerce trading system. The threat model specifies three main aspects that require careful considerations when designing security services for an ad hoc m-commerce trading system, namely constraining participation, sharing trading experience and sharing expressions of trust among traders. Possible countermeasures that can be used to address or at least mitigate each category of threats and vulnerabilities, and can be implemented in a way that can suit with the security requirements, and the nature and characteristics of an ad hoc m-commerce trading system are identified, evaluated and critically analysed. (Chapter 3)

4) The design of a novel ad hoc m-commerce trading system framework is proposed that specifies a standard set of core services and functionalities for m-commerce trading conducted online and wirelessly outside established computer infrastructure. The framework also serves as a basis for addressing the major security issues involved in trading wirelessly among computing nodes in a dynamic network and in the absence of a network service provider. The framework also presents an abstract architecture for an ad hoc m-commerce trading peer. (Chapter 4)

5) A trading model for an ad hoc m-commerce trading system was formulated. The trading model presents the main steps and processes involved in a representative kind of ad hoc m-commerce transaction. (Chapter 4)

6) The design and security analysis of a novel identity support scheme for a security and trust service in ad hoc m-commerce trading systems [119] that aims to protect traders from identity-related threats and information-related threats. (Chapter 5)

7) The design and security analysis of a fully distributed reputation system that aims to provide high availability, efficient retrieval and reliable reputation information for traders in such a loose and dynamic trading community. (Chapter 6)

8) The design and security analysis of a novel group membership service [118] that aims to constrain ad hoc m-commerce trading system participation to only traders that are regarded as trustworthy by other traders in the trading system. (Chapter 7)

9) A security warning scheme that aims to improve the security of an ad hoc m-commerce trading system by allowing traders to share their knowledge about suspected misbehaviour or malpractice by other traders in the trading system. (Chapter 8)

10) A formal verification of ad hoc m-commerce trading system processes using the SPIN model checker that aims to verify certain safety properties. (Chapter 9)

1.5 Thesis Outline

This chapter provides an introduction to the entire research. The remainder of this thesis is organized as follows. Chapter 2 discusses the concept of mobile commerce over ad hoc wireless networks (ad hoc m-commerce), its characteristics, main entities, functional components and target applications, as well as its potentials and challenges. In order to facilitate discussion, a critical analysis of m-commerce and ad hoc wireless networks is presented and their definitions are clarified. Also, their characteristics, current implementation and functional elements are explained, and their general requirements and issues are outlined.

Chapter 3 defines a threat model that specifies possible threats and vulnerabilities that can subvert the functionality and dependability of an ad hoc m-commerce trading system. Based on the threat model, three major security requirements for securing an ad hoc m-commerce trading system are identified, namely constraining participation to fit parties, sharing experience of trading by parties and sharing expressions of trust in the tradeworthiness of parties.

Chapter 4 describes and presents a general conceptual framework that includes a standard trading model and an abstract architecture for an ad hoc m-commerce trading system.

Chapter 5 presents the design of an identity support scheme for a security and trust service for an ad hoc m-commerce trading system and a security analysis of the proposed identity support scheme.

Chapter 6 discusses three key issues in designing an effective reputation system for ad hoc m-commerce trading systems, namely reputation information storage, integrity maintenance and reliability assurance. The design of a fully distributed reputation system that addresses the three key design issues and a security analysis of the proposed reputation system are then presented.

Chapter 7 presents the detailed mechanisms for managing group membership in an ad hoc m-commerce trading system. The design of such membership service is then presented and analysed.

Chapter 8 discusses the importance of having a mechanism to allow traders to share their knowledge about suspected misbehaviour or malpractice using warning or alert messages. A detailed security warning scheme for an ad hoc m-commerce trading system is then presented.

Chapter 9 presents the formal verification of ad hoc m-commerce trading system processes using the SPIN (Simple Promela Interpreter) model checker.

Finally, Chapter 10 summarizes the presented work and concludes it by discussing its limitations and outlining issues that remain open for future work.

Chapter 2

Background

2.1 Introduction

This chapter discusses the concept of ad hoc m-commerce, its characteristics, main entities, functional components and target applications, as well as its potential and challenges. In order to facilitate discussion, a critical analysis of m-commerce and ad hoc wireless networks is presented and their definitions are clarified. Also, their characteristics and functional elements are explained, and their general requirements and issues are outlined. Current implementations of m-commerce primarily utilize infrastructure-based architectures [128], where users make use of a pre-established network service infrastructure supported by a network service provider. Though these kinds of architectures are relatively stable, straightforward to implement and can be made secure, network connectivity cannot be guaranteed in some places such as in rural areas and users often have to pay subscription fees in order to get connected to the network. In contrast, ad hoc architectures seem to be more attractive by providing a more convenient, flexible and low cost way of building m-commerce systems. Several well-known application types have been identified as suitable for ad hoc wireless networks, especially for emergency and rescue services and military operations [150],[37],[14],[57],[81]. However, ad hoc m-commerce holds promise as an emerging application area for ad hoc wireless networks. The last part of this chapter summarizes the potential of ad hoc m-commerce as the motivation for this PhD research, as well as identifying a number of challenges that implementation of it must be overcome.

2.2 Mobile Commerce (M-Commerce)

2.2.1 Definition

Various definitions of the term "m-commerce" have been offered [90],[89],[108],[159]. Some of these definitions seem to restrict m-commerce to online transactions that are conducted solely over a mobile telecommunication network and involve the transfer of monetary values. However, m-commerce transactions do not necessarily involve the transfer of money and can be conducted over other means of wireless communication. Furthermore, not all commercial transaction processes need to be carried out electronically as some transactions may be initiated electronically but completed off-line.

Therefore, in this thesis, m-commerce is taken to be a set of activities relating to the exchange of information, services and goods for either money or other information, services and goods, which is conducted fully or predominantly online over wireless technology using mobile devices. In a fully online transaction, all transaction processes, which include the advertising, negotiating, ordering, payment and delivery processes, are conducted electronically. In a predominantly online transaction, most transaction steps or the most parts of all steps like the advertising, negotiating and ordering processes may be done online but other steps or parts of them like payment and delivery processes may be done off-line.

2.2.2 Characteristics

M-commerce has several unique characteristics. Based upon different literatures [167],[147],[162],[89],[25],[50], the distinguishing characteristics of m-commerce can be summarized as follows:

Location and Motion Independence - The portability of mobile devices, the pervasiveness of mobile network access and widespread m-commerce service availability makes m-commerce transactions possible irrespective of where the user is or whether the user is moving.

Localizability - Technologies like Global Positioning System (GPS) enable users and mobile network operators to locate each other and to tailor access to commerce services specific to their location.

Personalisation - Mobile devices are normally not shared among users. This enables users to customise these devices to their individual commerce service requirements.

2.2.3 Requirements

Although different m-commerce applications have different requirements [164],[161],[30], in general m-commerce applications have the following requirements:

- Adequate quality of service in the wireless network to avoid delays that may affect the performance of m-commerce applications.
- Reliability in the wireless network so that users can access m-commerce applications, even under varying degrees of network failure.
- Ability to roam across multiple heterogeneous wireless networks so that users can access m-commerce applications independent of their location.
- End-to-end security supported so that trading parties can trust the other trading parties to provide their service at an acceptable level of risk.
- Convenience and usability so that users can perform m-commerce transactions easily and unproblematically.

2.2.4 Issues

Even though m-commerce has created a new way of conducting business and led to the design and development of new services, there are still issues that need to be taken into consideration for the success and further development of m-commerce. The issues are listed below:

1. Mobile Devices

Mobile devices have limited battery lifetimes and thus there is a limited time during which they can operate without recharging their energy resources. This limitation may restrict mobile devices from performing some more complex and energy intensive computations because such computations would require and consume substantial amounts of power and thus would drain the battery faster. Moreover, the use of a wireless medium for data transmission can make the battery life shorter as it consumes significant energy [153]. Therefore, mobile devices cannot be expected to be always available in a network like stationary computing devices. Users may cut their wireless connection to the network in order to reduce power consumption or the battery of a mobile device could lose all its charge. The main exception to mobile computers being seriously power constrained by their limited battery lifetimes are mobile computers designed to be carried by vehicles with petrol or diesel engines. However, their mobility is constrained by where these vehicles can travel

and how far distant the nearest refueling station is. So they will be regarded as a special case.

2. Wireless Networks

Wireless networks have some constraints that could limit the reliability and capability of m-commerce applications.

- Bandwidth

  Wireless networks have limited bandwidth. Although they are expected to come to have higher bit rates, the transmission rates in many wireless networks such as in cellular or satellite networks are still low as compared to wired networks [153]. This is partly because wireless communications are rather more error prone and require much redundancy in the channel coding of the payload.

- Connectivity

  Wireless networks are less reliable because they are more prone to network disconnections. Factors that can cause network disconnections include lack of cellular or satellite network coverage, radio interference, changes in the signal strength and the limited battery lifetime of mobile devices. In some m-commerce applications such as mobile financial and mobile entertainment software, continued network connectivity is one of the most important requirements as discontinued connections may affect the outcome of transactions.

- Variant tariffs

  Different networks have different network access charges. In some networks, network access is charged per connection-time for example in cellular telephone services, while in some other networks, it is charged per message or per session or per transaction and so on [153],[160].

- Asymmetric Communications

  Channels in wireless networks may be asymmetric [159]. The bandwidth available for uploading data may be rather lower than the bandwidth available for downloading data.

3. Security

There are at least three aspects of security that need to be considered: the security of mobile devices, the radio communication channel and payment systems.

- Mobile devices

  Mobile devices, especially high mobility devices, are prone to be stolen, lost or accidentally damaged due to their small size and portability. Since these devices are highly personalized and are often used to store confidential user information, it is important to protect not only the data that is transmitted through the network but also the data that is stored on the device itself. However, due to their limited computation capabilities and memory size, it is demanding to employ high security schemes on those devices.

- Radio Communication Channel

  Performing electronic transactions over wireless networks is inherently insecure as compared to wired networks [165]. A radio communication poses additional security vulnerabilities. Its broadcast nature makes it easier for attackers to intercept and spoof on going traffic if no security mechanisms such as communication encryption are employed. There are three common types of attacks: disclosure attacks, integrity attacks and denial of service attacks [9]. Disclosure attacks are where the confidentiality of data transmitted over the network is compromised by its contents being revealed to other parties that are not involved in the communication by means such as eavesdropping, masquerading, traffic analysis and so on. Integrity attacks are where the contents of a message being transferred over the network are altered or deleted or reused without permission. In a denial of service attack, access to the network is made impossible by jamming the radio signal. In addition to security attacks, frequent handoffs and disconnections due to path loss, fading and interference can degrade the service levels of security services. Also, the mobility of mobile devices introduces an additional difficulty in identifying and authenticating devices in the network.

- Payment System

  M-commerce applications, especially those involving mobile payments require secure information exchange as well as safe electronic financial transactions. Without a secure payment system, neither customers nor merchants may be prepared to engage in monetary m-commerce transactions. For instance, both parties that are involved in a financial transaction would want to authenticate each other before committing to any payment. Also, they would want assurance on the confidentiality and integrity of the sent payment information as well as effective support for non-repudiation to prove that a transaction has happened.

4. Social, Ethical and Legal Issues

To avoid risks such as legal actions, brand damage and so on, parties that are involved in m-commerce transactions need to ensure that all m-commerce activities such as services, transactions, payments and so on, comply with government and industry regulations as well as their internal policies. Below are some of the regulatory issues that need to be addressed:

- Data protection and data breaches

  Regulations related to the protection of subscriber data, identity theft and the reporting of data breaches.

- Digital rights

  Digital content such as music, clip art, videos and so on are subject to Intellectual Property (IP) constraints such as copyright, trademarks and so on.

- End-user privacy

  Regulations related to consumer protection and privacy laws in order to ensure consumer privacy is not violated.

- Child protection and legality

  Regulations related to offering, accessing and purchasing of adult related content, products and services. For example, some adult content is illegal, or age verification may be required before accessing or purchasing any adult related content, products or services.

- Money laundering and gambling

  Regulations related to electronic money transfers, money trafficking issues and so on.

2.3 Infrastructure-Supported M-Commerce

2.3.1 Functional Components

M-commerce systems involve various disciplines and technologies, and can be divided into six components [77], as illustrated in Figure 2.1.

Mobile Commerce Applications - There are a wide variety of existing and potential m-commerce applications [69],[166],[128],[18],[43]. These applications can be classified into several classes as listed in Table 2.1 (page 17).

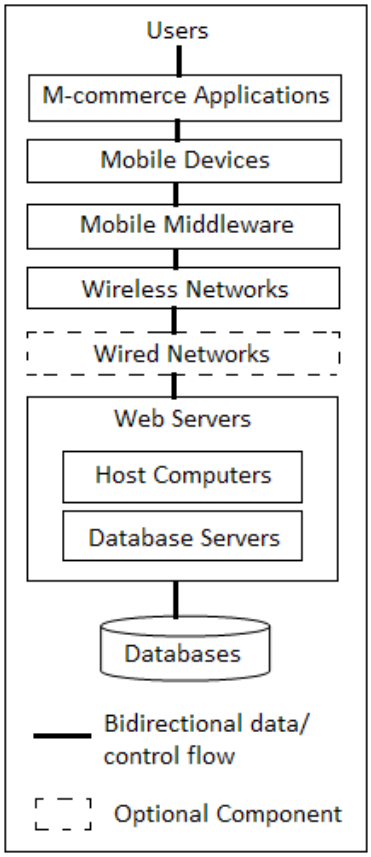


Figure 2.1: Main functional components in an infrastructure-based mobile commerce (Adopted from Hu, Lee and Yeh, 2008).

Mobile Devices - Mobile devices with sufficient memory, computing power, storage and display capability, as well communications functionalities enable consumers to engage in m-commerce transactions regardless of time or location. Mobile devices such as smart phones, laptop computers, tablets and so on are now equipped with communication interfaces that can support a variety of network communications including Bluetooth, Wi-Fi and wireless WAN access [166]. These devices have also been augmented with features like location and video streaming support, inbuilt cameras, barcode reader software and so on to support a wide range of m-commerce applications.

Mobile Middleware - Mobile middleware refers to an enabling layer of software that joins together different mobile applications, networks and technologies via a common set of interfaces [128],[101]. It enables m-commerce applications to function with greater reliability and capability so as to provide a uniform and user-friendly interface as well as better response times.

Wireless Networks - Networking support from wireless networks plays an important role in m-commerce systems as mobile users need to go through a wireless network connection in order to perform m-commerce transactions via m-commerce applications on their mobile devices. There is a broad range of wireless networking

Class of Applications	Examples
Information	News and Weather
	Maps and travel related information
	Logistical information
	Emerging service information
Entertainment	Sports, Games and Gambling
	e-Books, e-magazines
	Movies, images and music
	Streaming media
Commercial	Banking
	Mobile Auctions
	Booking and Reservation
	Online shopping and stock trading
Marketing and Advertising	Mobile coupons and promotions

Table 2.1: Classes of m-commerce applications

technology that is available to provide networking support required by m-commerce systems which includes operator-driven networks like General Packet Radio Service (GPRS), Enhanced Data rates for Global Evolution (EDGE) and Universal Mobile Telecommunications System (UMTS), as well as wireless LAN (WLAN) via Wi-Fi and wireless PAN via Bluetooth [82],[140],[18],[95]. K_a band satellite wireless is not competitive with terrestrial wireless because of latency, speed, cost and energy usage disadvantages quite apart from deployment issues with satellite dishes to access satellite wireless.

Wired Networks - Although a wired network is an optional component in m-commerce systems, most computers or servers that are used to execute m-commerce processes and store all the transaction related information usually reside on wired networks [166].

Host Computers - Host computers are computers or servers such as web servers, database servers and so on, that are used to process and store m-commerce transaction related information.

2.3.2 Main Entities

Generally, there are four main entities in m-commerce systems [13].

1. Customer

The person who is mainly mobile and makes use of the m-commerce system for

the purpose of obtaining and paying for contents, products or services offered by merchants or content/service providers.

2. Merchant or Service/Content Provider

The entity that provides the contents, products and services to customers either directly or through a mobile network operator.

3. Mobile Network Operator

The entity that provides the network connectivity that links customers, merchants and financial institutions.

4. Financial Institution

The entity that provides the payment mechanism such as Electronic Funds Transfer at Point of Sale (EFTPOS) or Automated Teller Machine (ATM) service.

2.3.3 Entities Relationships in the M-Commerce Value Chain

Entity relationships in an m-commerce value chain can vary depending on the types of transactions. For example, a relatively simple transaction such as buying a soft drink from a vending machine would only involve a customer, mobile network operator and its vending machine that supplies soft drinks [77], as illustrated in Figure 2.2. In this scenario, the customer has relationships with both the mobile network operator and the vending machine. The mobile network operator charges the customer for using its service to purchase the soft drink by adding the cost of the soft drink to the customer's mobile phone bill.

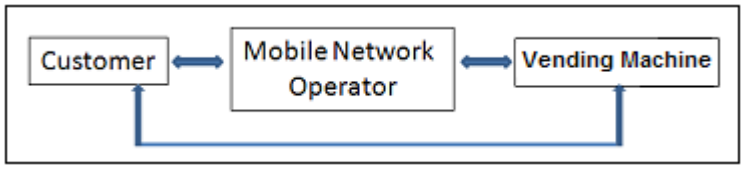


Figure 2.2: Relationship involving customer, mobile network operator and vending machine.

A more complex m-commerce transaction might involve a financial institution or cryptocurrency ledger server [110]. In this scenario, the customer has a relationship with the mobile network operator, the financial institution and also the merchant [77], as shown in Figure 2.3. The mobile network operator enables the transaction to take place by providing mobile services to the customer. To purchase products, the customer needs a relationship with the financial institution that handles the

transaction payments. The customer will also need a relationship with the merchant for the goods purchased.

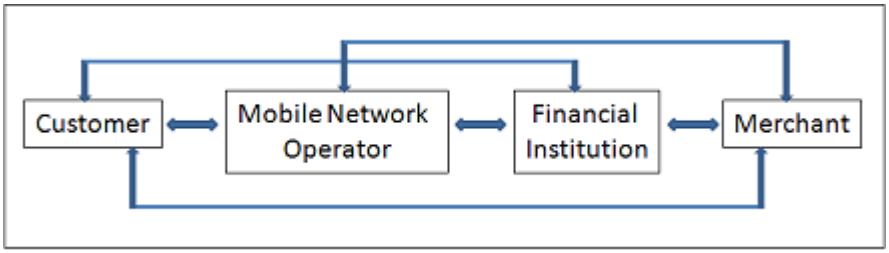


Figure 2.3: Relationship involving customer, mobile network operator, financial institution and merchant

Another scenario is a relationship between a customer and mobile network operator and also a relationship between a network operator and content provider [165], as depicted in Figure 2.4. The customer obtains the content or service from its provider through its mobile network operator and pays the operator who remunerates the content or service provider in turn.

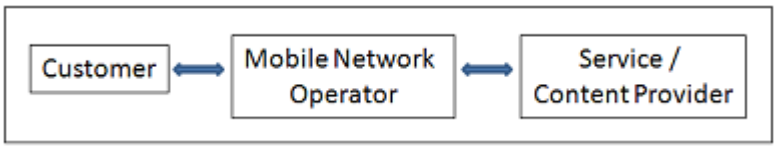
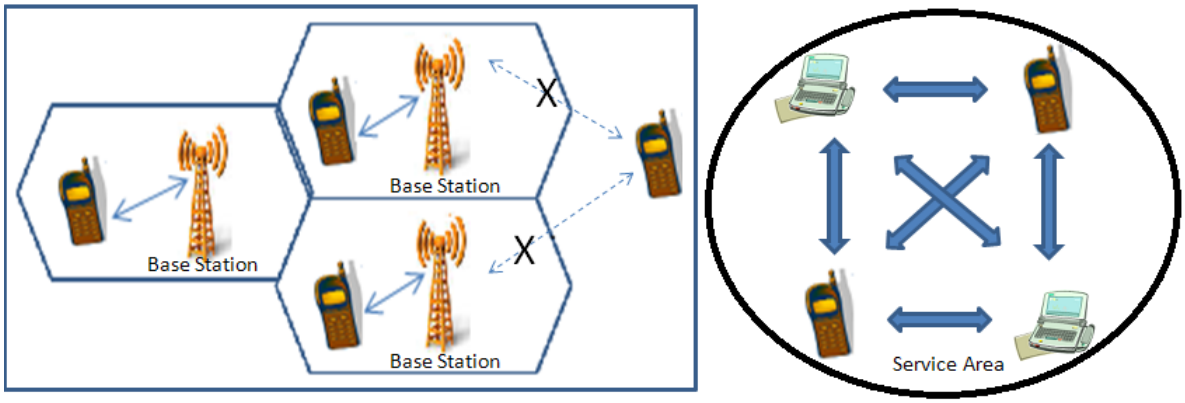


Figure 2.4: Relationship involving customer, mobile network operator and content provider

2.4 Ad Hoc Wireless Networks

2.4.1 Definition

An ad hoc wireless network is a type of wireless network that does not rely on a fixed infrastructure such as a base station, or centralized administration in order for the nodes to form the network and communicate with each other [103],[131],[150]. It is formed when there is a need (impromptu) to accomplish a specific task among nodes that are within direct or indirect communication range with each other, using available resources on hand [28]. The nodes are responsible for discovering each other and organizing themselves to create a virtual communications infrastructure to route and disseminate data among them. Figure 2.5 shows the difference between two wireless network architectures; infrastructure-based wireless networks and ad hoc wireless networks (infrastructure-less).



(a) Infrastructure-based Wireless Network (b) Ad Hoc Wireless Network

Figure 2.5: Infrastructured and infrastructure-less wireless networks

Nodes that form an ad hoc wireless network may be mobile or static. One type of example of an ad hoc wireless network that consists of mobile nodes such as laptops, smartphones or tablets is called a Mobile Ad Hoc Network (MANET) [14],[32]. Stationary nodes are often found in Sensor Networks [37],[106], where sensors typically do not move once deployed. For example, the deployment of specialized wireless sensor nodes at selected high risk areas in a forest for early detection of fires. Sensor networks can also be linked to the Internet to feed real-world information to Internet of Things (IoT) applications. For example, sensors in the home will enable users to interact with their smarthome applications to manage and control their home security and appliances remotely using their mobile devices. More details about IoT will be discussed in Section 2.4.4.1.

Ad hoc wireless networks can either be standalone networks or may also be connected to a larger network such as the Internet via an Access Point (AP) [171],[88],[12]. In ad hoc wireless networks, some or all nodes act as routers as well as being hosts [78]. The nodes perform the function of a host when transmitting and receiving data and act as a router when routing data packets among other nodes in the network [109]. Nodes within ad hoc wireless networks can communicate directly with each other if the destination node is within the sender's transmission range. For instance, in Figure 2.6, node B is within the node A's transmission range. Therefore, node A and node B can communicate directly with each other. However, if the destination node is outside the sender's communication radius, other nodes will need to be used as intermediate hops to relay packets until the destination node is reached. Hence, an ad hoc wireless network is sometimes called a multihop wireless network. For example, node C in Figure 2.6 is out of node A's transmission range; thus in order for node A to communicate with node C, node B will need to act as a router to pass on data packets so they can reach node C.

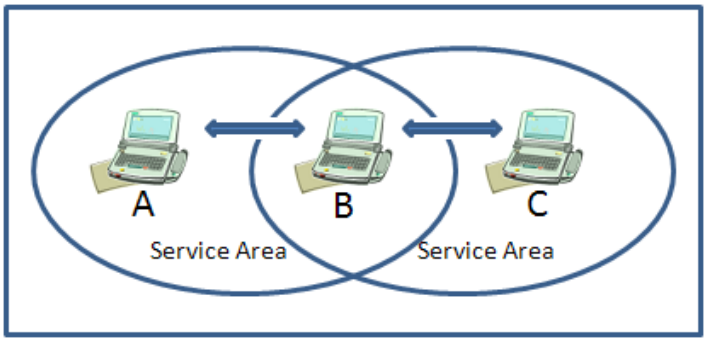


Figure 2.6: Basic structure of an ad hoc wireless network

There are various wireless access standards that support the ad hoc networking paradigm, which include the following [39]:

- IEEE 802.16 Standard, also known as WIMAX, refers to a series of specifications developed by the IEEE to support high-speed wide range wireless broadband or metropolitan area network (MANs).
- IEEE 802.11 Standard, also known as WiFi, refers to a group of specifications developed by the IEEE for high-speed medium range MANET or wireless LANs (WLANs).
- IEEE 802.15.1 Standard, also known as Bluetooth, is a wireless access specification for exchanging data over short distances and building personal area networks (PANs).
- IEEE 802.15.4 Standard, also known as Zigbee, is a wireless access standard that is designed for short-range low data rate networks. ZigBee has a defined rate of 250 kbit/s, that makes it ideal for intermittent data transmissions from a sensor or control device.
- WiFi Direct is a set of services for the use of WiFi that enables devices to connect to each other without the use of an access point.

2.4.2 Characteristics

An ad hoc wireless network has certain characteristics that distinguish it from other types of network. They include the following [32],[150],[70]:

Dynamic Network Topology - In an ad hoc wireless network, nodes can leave or join the network freely and are often dynamically and arbitrarily located. Furthermore, the topology of the network can change as nodes are free to move from

one location to another. This can result in route breakages where an optimal communication path at a given point in time cannot be maintained and might not be available for use at another period of time [179].

Fluctuating Link Capacity - Wireless communication has a higher bit error rate (BER) as compared to wired networks [109]. In ad hoc wireless networks, more than one end-to-end path can use a given link which can cause several sessions to be disrupted if the link breaks. In addition to that, the reliability of a wireless channel is likely to be lower than wired ones because wireless channels suffer from path loss, fading and also interference [133].

Self-Organization - The network can be created on the fly without the need for any system administration [158]. Nodes are able to detect the presence of other devices and perform the necessary handshaking to allow communication, dissemination of information and also sharing of services among them. If one node moves in or out their communication range, the other nodes in the network should be able to re-configure the topology of the network.

Distributed Operations - Due to the dynamic topology and infrastructure-less architecture of an ad hoc wireless network, the protocols and algorithms used for routing are designed in a decentralized manner so that nodes are capable of configuring and organizing a network without any central administration or management.

Battery Powered - Nodes in ad hoc wireless networks such as laptops, smart phones and tablets are often battery powered mobile devices. Therefore there is a limited time during which they can operate without changing or recharging their energy resources.

2.4.3 Applications

At present, there are a number of (potential) applications for ad hoc wireless networks, ranging from large scale and highly dynamic to small scale and static networks [58],[103],[150],[62]. These kinds of applications as depicted in Table 2.2, are normally used in places that have little or no communication infrastructure available such as in the battlefield areas, or in situations where the existing infrastructure is costly, problematic or inconvenient to use, such as in disaster zones. They are also suitable to be used in conditions where only a temporary network connection is required to accomplish a specific task, for example to accomplish a spontaneous collaborative task in a conference or campus setting. In other situations, for example in metropolitan areas, they can be used to provide quick and easy wireless network deployment or for network coverage extension.

Class of Applications	Examples
Military Operations	Military communications
	Automated battlefields
Emergency and	Search and rescue operations
Rescue Services	Disaster recovery
	Policing and fire fighting
Car Networks	Traffic or weather updates
	Accidents or road conditions warnings
	Taxi or car rental networks
	Inter-vehicle networks
Conference or	Virtual classrooms
Campus setting	Information sharing among participants or students
	Extension to a larger network, e.g. Internet
Sensor Networks	Smart Home applications
	Body Area Network (BAN)
	Data tracking of animal movements
	Environmental monitoring, e.g. bushfires detection
	Natural disaster forecast, e.g. earthquake or tsunami

Table 2.2: Examples of ad hoc wireless networks applications

Although there is still no silver bullet application for ad hoc wireless networks [122], ongoing research in ad hoc wireless networks is now maturing, especially within the IETF's MANET working group [80]. This will help to stimulate further achievements in this area as the research facilitates new applications to be created. Furthermore, as the trends are now moving towards 'anytime, anywhere' communication, commercial applications such as mobile commerce will be intriguing future applications of ad hoc wireless networks.

2.4.4 The Future

Ad hoc wireless networks have been in use since the early seventies, mainly for military operations [173],[41],[107]. Since then, a significant amount of research has been done in this area and wider interest has continued to grow among the research community over the past few years [122],[131],[97],[57]. Much of this research [103],[57],[152],[60],[49] shows that an ad hoc wireless network is a promising technology for future wireless communication networks that offers a flexible, convenient, easy to deploy and inexpensive solution.

With the current trend in communication networks of increasing demand for pervasive and ubiquitous computing, future living environments seem to require a com-

munication network that is able to self-organize, as well as reconfigure itself to keep people connected wherever they go or whenever the need arises. An ad hoc wireless network, with its self-organization and self-configuration characteristics is able to provide such a kind of network connectivity at any time or locations, even in undeveloped remote areas of the world. In addition to that, its inherence flexibility, lack of infrastructure, low cost of implementation, as well as ease of deployment and maintenance will make it an essential part of future wireless communication networks, serving as a complement to existing infrastructure networks to provide seamless access to information resources and services [173].

In the near future, it is likely that ad hoc wireless networks will be more widely used in its present application domains such as battlefield areas, emergency operations or sensor networks. This is due to the advancement of mobile devices that are getting smaller, cheaper, with longer lasting batteries, more functions and more commonplace [103], as well as rapid improvement in wireless communication technologies [103],[173]. For instance, many mobile devices today especially mobile phones are already equipped with Wi-Fi or Wi-Fi Direct or Bluetooth capability, as well as multimedia support. In addition to that, WiFi technologists are now working on 802.11ah (also called as Low-Power WiFi), a new revision of Wireless LAN (WLAN) standard that will allow wireless access operating at sub 1 GHz license-exempt bands [87],[151]. 802.11ah is intended to support large scale and cost-effective wireless networks, as well as the IoT. With 802.11ah, the WiFi transmission range can be extended much longer than the current 802.11 WLAN standards, the throughput can be significantly improved and the energy consumption of the battery-powered devices can be reduced [151].

As a consequence, there is a potential for ad hoc wireless networks to be used to facilitate new business opportunities for the users with profitable commercial applications, enabling ad hoc wireless networks to move from military or emergency contexts to the commercial world. It will be possible for ad hoc wireless networks to create novel commercial application opportunities that will shape its future, like the Internet that existed for more than 20 years before the World Wide Web came along and has been very widely used ever since. However, the realization of this commercial world still requires a number of issues related to mobile devices, protocols, trust and security and also other important services to be addressed appropriately [103]. In addition to that, appropriate business scenarios and their possible applications need to be identified.

2.4.4.1 Internet of Things

The Internet of Things, also known as IoT is an emerging technology that was first identified some 15 years ago by Kevin Ashton, the cofounder and executive director of Auto-ID Center at Massachusetts Institute of Technology (MIT) [20]. The term IoT has been defined in many different ways [53],[87],[35],[169]. A common definition of IoT that has gained acceptance among experts is "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes and virtual personalities. These same things use intelligent interfaces and are seamlessly integrated into the information network", as defined by the Internet of Things European Research Cluster (IECR) [169]. Although there are numerous definitions of IoT, the role of the IoT remains the same, which is to enable all things in the physical world with the power to communicate to be connected with each other in a useful way anytime, anywhere, using any network or service.

From a technological perspective, IoT refers to the concept where all the physical things (objects) that utilize embedded technologies such as Radio Frequency Identification (RFID) tags, sensors, actuators and etc, can communicate and share information with each other and also with the environment in a useful fashion and make themselves recognizable, all via the Internet. The things, in the IoT scope can be everyday objects such as home or electronic appliances, farming equipment, medical instruments, cameras, vehicles, industrial equipment and many more. They can also include living organisms such as people, plants, animals and so on. The enabling technologies that will allow things to communicate with each other include various types of wired and wireless connections such as RFID, WiFi, Zigbee, GSM, GPRS, 3G, 4G, and etc. With the IoT, the physical world will be integrated with the digital or virtual world to produce one big information system. This kind of interconnection will enable a new form of communication among things and people, among things and the environments, or infrastructures and also among things themselves, which will significantly change the way people interact with their surroundings and then transform how they live and work.

The IoT is currently being deployed in a wide variety of areas, which include homes, cities, businesses, healthcare, transport and agriculture. One example of the deployment of IoT applications in cities is the smart parking system, where sensors are deployed in parking areas to enable users to check the availability of parking spaces in the city. Another example is in dairy cattle farms, where sensors are implanted in the ears of cattle to enable farmers to track the movement of their cows and also to monitor their health in order to sustain their wellbeing. In 2013, around 9 billion smart devices were connected via networks in the world [67] and it is predicted that

there will be more than 50 billion connected devices by 2020 [53]. In line with this progress, most of the governments in Europe, Asia and also the Americas are now considering the IoT as an area of innovation and evolution [56]. It is expected that this development will lead to a new revolution of applications that will generally improve people's lives and also create many new business opportunities.

2.5 Ad Hoc M-Commerce

2.5.1 Definition

Unlike infrastructure-supported m-commerce, ad hoc m-commerce takes place between 2 or more mobile devices that are in the vicinity of each other and use an ad hoc wireless network as a communication medium. These devices are peers that typically have similar capabilities. Trading can be initiated by any peer with networking capability and does not require any third party infrastructure to manage it. Its participants communicate and cooperate by utilizing each other's resources without relying on any support provided by a network service provider in order to accomplish the transaction or any other tasks. Thus, in this thesis, ad hoc m-commerce is viewed as self-configured and self-organized m-commerce trading that is conducted via ad hoc wireless networking.

2.5.2 Characteristics

Due to the unique characteristics of m-commerce and ad hoc wireless networks, ad hoc m-commerce can be said to have the following characteristics [117]:

No network service provider - Because ad hoc wireless networks lack a network service infrastructure and are self-organized, a network service provider cannot be relied upon to be present to provide security or payment services whenever nodes engage in m-commerce transactions. Unlike GPRS or EDGE or UMTS mobile networking, there is no telecoms operator available to underpin m-commerce transactions as a value added service to the basic communication service.

Limited communications scope - IEEE 802.11 (Wi-Fi) and Bluetooth have limited communication ranges. The effective range for Bluetooth is 10m although it can extend to a 100m radius [24] while the transmission range for Wi-Fi is 100m in buildings and can cover up to a 300m radius in open spaces [157]. Therefore, such networks are suitable for short range node to node communication. While nodes can bridge gaps by routing information over multiple hops via nodes in between

themselves and so extend the range of such networks, those ad hoc connections via intermediaries may not be long lasting and may not be available much of the time due to the dynamic topology of the network and the limited willingness of nodes to expend scarce energy resources to route communications for others. So, much of the time it is not to be expected that there can be a suitable third party service available that is trusted by communicating peers to support security and/or payment services in real-time among the peers.

Limited time online - Due to limited battery lifetimes and the mobility of mobile devices as well as frequent network disconnections, there is a limited time during which these devices can be online, which restricts them from engaging in lengthy and complex transaction processes. This means that transactions need to be completed in a fairly short period and only comprise a few simple stages if they are to have a good chance of success. Therefore, realistic transactions must not involve long sessions or complex processes. Since mobile devices are peers and these devices themselves can become the service or information provider as well as the consumer, the limited time online restricts a trusted service or information provider from providing ubiquitous services or information to other devices in the network. Moreover, it is not realistic to have long-term third party security or payment services available all the time in the network. However, it would be possible to have intermittently available third party services although often not in real time.

Spontaneous decisions in Ad Hoc Settings - The self-organizing characteristic of an ad hoc wireless network allows users that are equipped with mobile devices and suitable software to spontaneously engage in m-commerce transactions when the need arises while they are on the move. For example, passengers in two cars near each other in slow traffic can establish an ad hoc wireless network connection and carry out m-commerce transactions while within range of each other.

Low cost - An ad hoc wireless network provides a low cost wireless connection [57] for users to engage in m-commerce transactions as it operates using a license free frequency band. Buyers or traders can save on network access charges as there is no subscription fee required to access the network. In addition to that, no additional device is required to perform m-commerce over an ad hoc wireless network as mobile devices that form the network will utilize their local resources and also resources on other devices that are in their proximity in order to accomplish the transactions. The overhead of purchasing or renting additional devices such as special server(s) that are used to process the transaction as well as to store transaction related information is eliminated.

Confidentiality - Because no third party needs to be involved to realise network communication, the range of wireless communication is limited, and transactions

may be conducted on the move, ad hoc m-commerce is suitable for confidential commercial exchanges where the trading parties do not wish their exchange to be known or guessed at by external parties. For example, two or more parties may exchange their confidential corporate or business information such as business proposals, marketing strategy information deals and so on while they merely pass close by each other.

2.5.3 Functional Components

It seems that only the first four functional components in Figure 2.1 as discussed in Section 2.3.1, are required to construct an ad hoc m-commerce system [117], as shown in Figure 2.7. This is due to the fact that only an ad hoc wireless network is used as a means of wireless communication to carry out m-commerce transactions and such a network is often spontaneously and temporarily created when the need arises among mobile devices that are in close proximity to each other without relying on any infrastructures.

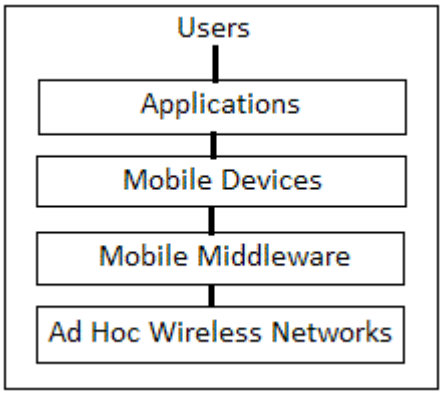


Figure 2.7: Four main functional components in an ad hoc m-commerce system

2.5.4 Main Entities

Since ad hoc m-commerce transactions involve only mobile devices that are peers and have no guarantee of infrastructure support from a network service provider, there are only two essential entities involved in the trading system.

1. Customer or Trader

The customer is the party who may be mainly mobile that makes use of ad hoc wireless networks to buy digital contents, products or services offered by the seller or to trade contents, products or services for others.

2. Seller or Trader

The seller is the party that provides the digital contents, products or services directly to customers or buyers via ad hoc wireless networks for money or who trades contents, products or services for others.

2.5.5 Entities Relationship in the Ad Hoc M-Commerce Value Chain

As different type of transactions would have different entity relationships, there are several possible essential entity relationships in the ad hoc m-commerce value chain. Figure 2.8 illustrates a relatively simple transaction involving two mobile devices. For example, two parties who are commuting in a train agree to exchange their electronic resources such as e-books while they are within transmission range of each other.

Figure 2.8: Transaction between two mobile devices

In a more complicated scenario where more than two mobile devices are involved in a transaction such as mobile auction or entertainment, the entity relationship can be illustrated as in Figure 2.9.

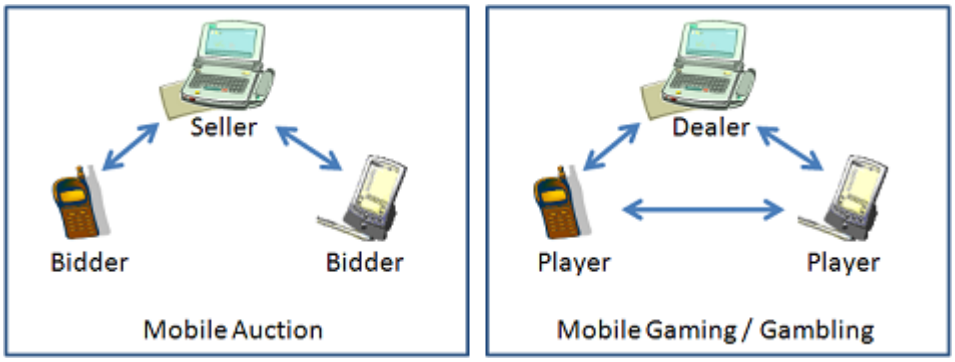


Figure 2.9: Transaction involving more than two mobile devices

Another scenario involving the formation of an ad hoc trading consortium among mobile users who are in the vicinity of each other and agree to band together for a

specific purpose, for example to make a collective purchase or to engage in group trading, the entity relationship can be illustrated as in Figure 2.10.

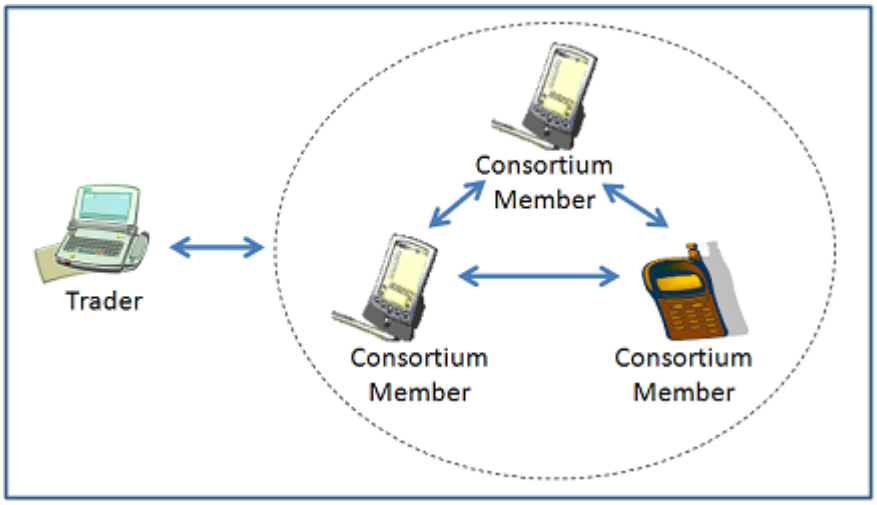


Figure 2.10: A group of individuals forming a consortium for trading

To represent different entity relationships in ad hoc m-commerce value chain, a generic view of ad hoc m-commerce transactions [117] is illustrated as Figure 2.11:

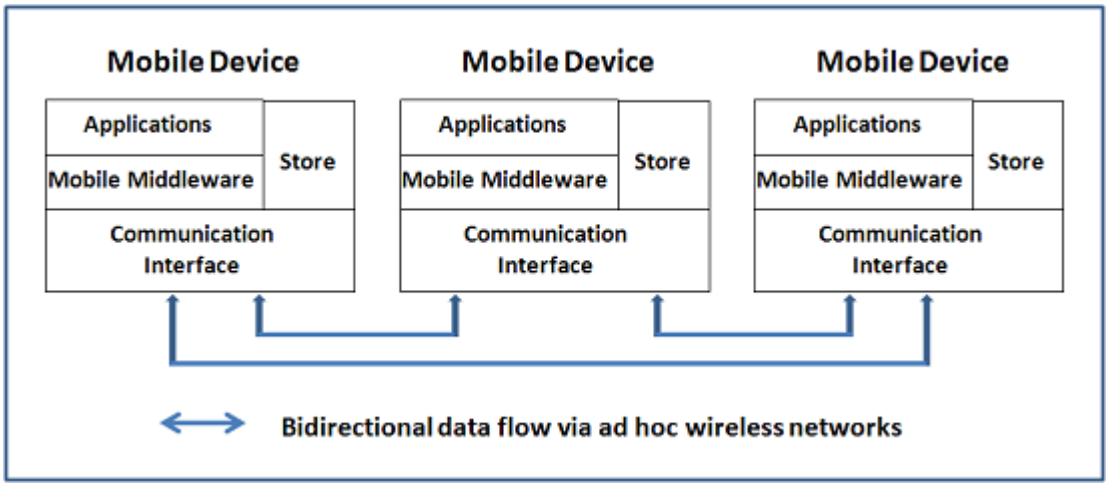


Figure 2.11: A generic view of ad hoc m-commerce transactions. The ad hoc m-commerce store will held certificates, attestations, offers, trading history and other transaction related information

2.5.6 Potential Applications

There are several distinct types of m-commerce transactions that can be carried out over ad hoc wireless networks:

Swapping of digital resources - Swapping of digital resources such as e-books, videos, music files etc. For example, two amateur ornithologist collectors who meet

by chance at an airport may agree to exchange some of their collectable bird song recordings.

Mobile Auction - The process of buying or selling certain items could be realised by an auction among a local group of people. An auction process can be created anywhere as soon as a group of at least three persons with mobile devices and appropriate software agree to participate. For instance, an auction could be created at a stamp collectors fair to sell a scarce stamp. This type of activity is amenable to short term participation by individuals and a rapid turnover in its membership as long as enough are usually present to create a critical mass of bidders. Multicasting among participants can disseminate bids and information about what is on offer.

Selling or Buying Items - A group of people in a neighboring area forms a trading community among themselves, for example a trading forum for selling second hand items. They can participate in the trading forum as either a seller or a buyer. The sellers advertise their items or resources to other members of the trading forum. They receive offers from potential buyers and answer the offer from potential buyers that they want to trade with.

Mobile Entertainment - Interactive gaming and gambling among small groups of people is another kind of application suited to ad hoc networking. Applications running on mobile devices realise the game or gambling scenario, manage its communications and handle the turnover in participants. For example, people on a train may play blackjack on their mobile devices over an ad hoc wireless network.

Confidential Exchanges - Two or more parties who meet at a certain place or pass in the vicinity of each other may agree to exchange their confidential information resources or services for a specific purpose as mentioned in the example given in section 2.5.2.

Transacting with Machines - Transactions that use mobile devices that are preloaded with E-cash [139],[114] to make payment at a vending machine, point of sales (POS), parking tolls and so on via technologies such as Wi-Fi and Bluetooth [127].

Consortium Trading - A group of individuals who are in the vicinity of each other and equipped with mobile devices and appropriate software can spontaneously form a consortium for a specific purpose. For example, a group of football fans at a football ground, band together as a single buyer to purchase a discounted group ticket in order to get a cheaper ticket for each of them to watch a match. Another example would be a group of football fans who form a consortium during a football match to engage in betting on the outcome with another group of football fans.

2.6 The Potential and Challenges of Ad Hoc M-Commerce

2.6.1 Potentials

With the following advantages of an ad hoc wireless network [28], it is likely that the concept of ad hoc m-commerce will be accepted and widely used in the not too distant future if it is designed carefully and all the issues are addressed appropriately [28]:

Independence from Central Network Administration - This will enable the participating parties that form the trading community to have full control on the network administration as well as group management and this task is distributed among them.

Self-configuring - This enables the traders to spontaneously engage in ad hoc m-commerce transactions when the need arises regardless of time or location.

Self-healing through Continuous Re-configuration - Ad hoc networks enable mobile devices to re-configure themselves to accommodate network disconnections due to network topology change.

Scalable - The ability to accommodate the addition of more nodes that are in close proximity with each other. This will enable a few or many traders to participate in a particular trading forum at the same time.

Flexible - Traders that are within communication range with each other can initiate or engage in ad hoc m-commerce transactions at any location or situation.

Cost Savings - This enables traders to engage in ad hoc m-commerce transaction without the need to purchase or install any additional devices such as special servers to support the trading process. Traders can also save a considerable amount of money on access fee charges as an ad hoc wireless network is a free wireless communication medium [103].

Rapid Setup Time - To form or join an ad hoc m-commerce trading community only requires traders to have mobile devices that are equipped with suitable networking capabilities such as Wi-Fi or Bluetooth capability.

Also, in the near future, with continuing progress in networking, software, sensor and other ICT technologies, as well as rapid advancement in devices' computation, processing power, storage and capabilities (particularly mobile devices), it is possible to envisage that the IoT will enable people to be online pervasively everywhere

by creating an environment of interconnected "smart" things. This kind of smart interconnection is expected to enable new ways of interacting, living and working, which could be lead to a revolution of new applications and services, as well as new business processes. Ad hoc m-commerce, with its low cost and self-organization characteristics that embody important features of IoT, could be one of the enabling technologies that will bring enhanced business opportunities to IoT markets.

Furthermore, there are a number of research studies that have been done to enable efficient and reliable data transmission in dynamic and intermittently connected networks, such as MANETs. These studies aimed to deal with issues related to frequent and persistent network disconnections and disruptions in such networks due to random node mobility, limited battery power and resources of mobile devices, short radio communication range and so on, have led to the concepts of Delay Tolerant Networking (DTN) and Opportunistic Networking [61],[175],[124],[112],[135]. These concepts have received a lot of attention from the networking research community as an evolution of MANETs [92], and are often interchangeably used by the researchers to refer to a new communication paradigm for wireless networks, where mobile nodes exploit any available resources in the network to enable them to communicate with each other, even in the absence of end-to-end connectivity between the sender and the receiver [29],[124]. In order to enable communication, a 'store-carry-and-forward' approach is employed to route messages towards their destination. For example, in a situation where a node has a message to be forwarded but a direct path towards the destination is unavailable as there is no other node in its communication range at that time, it will temporarily store the message and forward it later when an appropriate communication opportunity arises. It seems that with the studies done in the area of DTN and Opportunistic Networking, it is possible to deal with frequent network disconnections in ad hoc m-commerce trading systems, which could pave the way for more effective and reliable ad hoc m-commerce applications.

In addition to the above, the availability of cryptocurrencies such as Bitcoin, Litecoin, Dogecoin etc. could serve as a good example of a pure P2P system with very tough security requirements that have gained global interest and market traction in recent years [146],[72],[23]. A cryptocurrency is a kind of digital currency that uses specific cryptographic algorithms as a means of trade that allows transfer of value without the use of real life currency or going through a financial institution [110],[65],[72]. The first and most popular cryptocurrency is Bitcoin, which was developed by Satoshi Nakamoto in 2008. Bitcoin is a completely decentralized and purely P2P currency system that allows online payment to be made directly between two willing parties without the need for a central authority such as a financial institution [110]. Bitcoin users have full control of their transactions. They can make transactions without any involvement of a trusted third party or the need to

provide their real identity. However, they do need access to the distributed ledger or block chain in order to register Bitcoin transfers. Although to participate in its transactions does not require trust in anything other than the principles of the Bitcoin system and in the software used accurately implementing them, Bitcoin has gained large popularity and more real businesses are beginning to accept it. Studies [146],[66],[23] show that although the number of consumers or merchants who accept cryptocurrencies, particularly Bitcoins are still small, they have steadily increased. Like other emerging technologies, cryptocurrencies still have several important issues that require careful consideration before they can be widely accepted by consumers for daily commercial use, such as data protection and privacy, security, legal and government regulation issues [83],[66],[72]. Thus, there is a potential for ad hoc m-commerce systems to be widely accepted as a reliable alternative for m-commerce transactions if its trading software is designed carefully and its security issues are properly addressed.

2.6.2 Challenges

Performing m-commerce transactions over ad hoc wireless networks introduces additional issues and challenges. In addition to the issues discussed in section 2.2.4, ad hoc m-commerce has specific issues that require careful consideration in order to realize it in the real world. However, issues related to variant tariffs are not applicable to this kind of m-commerce trading as it operates using ad hoc wireless networks. Thus, no access fee is required to access the network. Other challenges that might constrain the success of ad hoc m-commerce include the following:

Transaction Management - Due to its unique characteristics such as lack of infrastructure, having a dynamic network topology and using resource constrained devices, it is a challenge to implement efficient transaction processing and updates in purely ad hoc wireless networks. Most solutions used in infrastructure based m-commerce depend on a client/server architecture [123],[76], where servers are used to handle all transaction processes and also store its related information. These servers usually are located within the wired network and configured with additional processing power, memory and also storage capacity. Mobile devices act as clients accessing the services provided by the servers [123],[76]. However, in ad hoc m-commerce, all devices are peers and normally have similar constraints on their resources, which will limit their capability to function properly as both servers and clients. The mobility of mobile devices that provide services (servers) to other devices is another important issue as the services are prone to becoming unavailable due to network disconnections. Also, the atomicity of a transaction can be difficult to enforce as network disconnections can cause a particular service in a transaction sequence to

fail and thus the transaction would be considered incomplete and be aborted [123].

Service Discovery and Delivery - A service discovery and delivery protocol enables devices to advertise their services to other devices as well as to discover services offered by other devices in the network. However, due to the unique characteristics and complexities of an ad hoc wireless network, existing service discovery and delivery protocols do not seem to suit the needs of an ad hoc wireless network, making them unsuitable for m-commerce oriented scenarios. Service advertisements and deliveries may need to be disseminated by a mix of a store and forward strategy as well as local multicasting to cope with intermittent online connectivity.

Gossip Protocols - A gossip protocol enables devices to periodically propagate and disseminate messages or information with a number of peers that are selected randomly from the available peers in the network [15],[26]. This type of protocol seems to suit the style of an ad hoc wireless network well as it is independent of network topology and allows messages to be propagated and disseminated slowly through the network without congesting the wireless medium. It also can be used as a kind of recovery strategy from message loss in multicast [26]. However, most gossip protocols assume that each node has sufficient resources available to store all the messages that it receives from its peers. This assumption may not be applicable to ad hoc m-commerce as nodes in such trading systems usually have serious limitations on their resources. Moreover, most gossip protocols require each node to know every other node in the network [59] and this requires the nodes to store and maintain a complete network membership table, which is not feasible in ad hoc m-commerce due to its dynamic group membership, irregular participation by trading parties and limited direct communication range.

Trust - Trust is essential in any online transaction as it helps the participating parties to feel confident to engage in such transactions by mitigating uncertainty and risks involved in the transactions, such as uncertainty about trading partners behaviour in fulfilling their transaction agreements [121]. However, as ad hoc m-commerce cannot rely on a network service provider to provide security services such as a Kerberos Authentication Server that can help to establish trust among trading parties in the network, traders have to rely on their peers in the network to provide trust evidence in order to evaluate other parties' trustworthiness. Yet, the nature of an ad hoc wireless network such as lack of infrastructure services, having a dynamic network topology, using resources constrained devices and so on, makes trust establishment in this network difficult to achieve.

Table 2.3 summarizes the potential of ad hoc m-commerce, and the challenges that must be overcome in its implementation in order to realize it in the real world.

No	Potential	Challenges
1.	With the advantages of an ad hoc wireless network such as independence of central network administration, self-configuring, flexible, cost saving and so on, it is likely that ad hoc m-commerce will be accepted and widely used if it is designed carefully, and all the issues are addressed appropriately.	Transaction Management - most solutions used in infrastructure based m-commerce depend on a client/server architecture, which is impractical in ad hoc m-commerce due to the nature of an ad hoc wireless network such as lack of infrastructure, having a dynamic network topology and so on.
2.	With continuing progress in networking, software, sensor and other ICT technologies, as well as rapid enhancement in mobile devices' computation, processing power and capabilities, it is possible to envisage that the IoT will be widely deployed in the near future. Ad hoc m-commerce, with its characteristics that embody important features of IoT, could be one of the enabling technologies that will bring enhanced business opportunities to IoT markets.	Service discovery and delivery protocols - due to the unique characteristics and complexities of an ad hoc wireless network, existing service discovery and delivery protocols do not seem to suit the requirements of an ad hoc wireless network, making them unsuitable for ad hoc m-commerce oriented scenarios.
3.	Research studies in the area of DTN and Opportunistic Networking [29],[124] shows that it is possible to deal with frequent network disconnections in ad hoc wireless networks, which could pave the way for more effective and reliable ad hoc m-commerce applications.	Gossip protocols - most gossip protocols require each node to know every other node in the network and have sufficient resources to store all the messages that it receives from its peers, which is not feasible in ad hoc m-commerce due to its dynamic group membership, irregular participation by trading parties and so on.
4.	The availability of cryptocurrencies such as Bitcoin, Litecoin etc is a good example of a pure P2P system with very tough security requirements that have gained global interest and market traction. Hence, there is a potential for ad hoc m-commerce systems to be widely accepted as reliable alternative for m-commerce trading if its applications are designed carefully and its security issues are addressed properly.	Trust - due to the characteristics of ad hoc m-commerce that cannot rely on a network service provider to provide its security services, and the nature of an ad hoc wireless network such as lack of infrastructures, having a dynamic network topology and so on, it is difficult to establish trust among traders in ad hoc m-commerce trading systems. Traders have to rely on each other's resources in order to make trust decisions.

Table 2.3: The potential and challenges of ad hoc m-commerce

Chapter 3

Security in Ad Hoc M-commerce Trading Systems

3.1 Introduction

Ad hoc m-commerce is an emerging way of conducting m-commerce transactions within infrastructure-less and dynamic network communities. However, since its trading activities are carried out over ad hoc wireless networks and as no network service provider can be relied upon to provide security services, this type of trading system is vulnerable to various types of attacks that can undermine its functionality and dependability. These include identity spoofing, Sybil attacks, man-in-the-middle attacks, unfair evaluations, collusions, misleading trade descriptions and so on.

To realize ad hoc m-commerce requires its security issues be properly understood and addressed to create sufficient confidence among traders to engage in such activity. A sufficiently trusted and secure trading environment will create a significant impact on traders' acceptance of ad hoc m-commerce applications. However, to design a security and trust service for ad hoc m-commerce trading systems is a challenging task due to its unique characteristics and also the nature of an ad hoc wireless network. Thus, it is important to understand and analyze the possible threats and vulnerabilities that could be present in such trading systems before designing or implementing any solutions in order to ensure the effectiveness of the solutions in addressing its security issues.

The remainder of this chapter is organised as follows. Section 3.2 discusses the role of security in online trading. Section 3.3 defines a threat model that specifies possible threats and vulnerabilities in an ad hoc m-commerce trading system. This section also discusses possible countermeasures that can be used to mitigate the threats. Section 3.4 determines three major security requirements for an ad hoc m-commerce

trading system, namely constraining participation, sharing trading experience and sharing expressions of trust. This chapter is concluded by Section 3.5.

3.2 The Role of Security in Online Trading

Security is vital in commercial transactions and more so in online transactions due to their virtual nature. Traders in popular online trading environments such as eBay or Amazon often have little information about the identity and behavior of the other parties involved in their transactions and about the quality of the goods or services at stake. This is partly due to the fact that they do not physically meet during these transactions, which usually take place between parties that do not know each other or have never met before. They also do not have the chance to see or try the products or services in advance before they purchase them. This makes the traders not only vulnerable to security attacks related to their online identity with respect to information being exchanged among them, but also to subversive behavior by their trading partners such as being given bogus or misleading information, which could subsequently expose them to transaction risks such as not getting what they have paid for or being cheated through non-payment. In the case of ad hoc m-commerce, the vulnerabilities are more crucial because the transactions are carried out over insecure ad hoc wireless networks and no network service provider can be relied upon to act as a trusted third party that provides security services.

Without adequate security, it is unlikely that traders will have the confidence to participate in online trading and thus, may refrain from participating in such transactions. One academic study found that 40% of Internet users provide incorrect information when they participate in online activities because they do not trust the security of the Internet [44]. Another academic study [132] based on a survey of US online shoppers found that security plays a major role in influencing customer's intentions to purchase online. Users are concerned about online security [63] and will only participate in online transactions if they can be assured that their transactions are low risk, the medium used to carry out the transaction is secure and reliable, and they will be able to validate the identity of the parties that they are going to deal with and gauge their trustworthiness, as well as verify the authenticity, integrity, confidentiality and non-repudiation of important information about their transactions.

3.3 The Threat Model

To create an environment that is secure and trusted to a sufficient degree to persuade traders to trade within ad hoc m-commerce trading systems, it is necessary to understand and analyze the threats and vulnerabilities present in such trading systems before designing or implementing any solutions because the threats determine the security measures. Thus, this section defines a threat model that specifies a set of possible threats and vulnerabilities in an ad hoc m-commerce trading system, in order to identify its security requirements and enable appropriate security measures to be deployed to address or at least mitigate those threats and vulnerabilities.

3.3.1 Security objectives

To be able to determine the most relevant and critical threats in an ad hoc m-commerce trading system and plan appropriate countermeasures for those threats in an effective way, this section specifies several key security objectives for such trading system, which include the following:

- Ensure tamper proof, non-interceptable and non-repudiatable messaging among traders with proof of authorship or origin.
- Keep transaction risks low which relate to misbehaviour of a trading party by provision of trustable identity support, reputation system and group membership schemes.
- Ensure the integrity and confidentiality of data stored in traders' local repositories.
- Support non-spoofable digital identities with digital certificates that enable authentication of a trader's credentials to be conducted and their identity verified.

3.3.2 Overview of Assets and Possible Threats

This section determines the key assets and possible threats in an ad hoc m-commerce trading system. Assets are the valuable resources of a system which can be tangible or abstract, while threats represent the potential violation of the security of a system that may cause some negative impact to the interests of users of that system that relate to those assets.

3.3.2.1 Assets

Assets and threats are closely correlated. It is unlikely for a threat to exist in a system if there is no target asset, because there would otherwise be nothing for a threat to target. To prevent a threat requires some sort of protection of assets. Thus, this section determines the key assets in an ad hoc m-commerce trading system that need to be protected to achieve its security objectives, as mentioned in Section 3.3.1 above. The assets are categorized as follows:

Trader's data which might be tampered with or disclosed to unauthorised parties. Thus, the integrity and confidentiality of a trader's data such as identity credentials, reputation reports, membership data, transaction contracts, testimonials and so on need to be assured at all times. In addition to integrity and confidentiality, the origin of data being exchanged among traders also need to be assured, so that no party can credibly deny having sent that data.

Trader's digital identity which might be spoofed by ill-intentioned parties. Thus, a trader's identity credentials in a digital certificate and crypto keys need to be protected from being stolen or compromised.

Trader's reputation which might be damaged due to identity spoofing, tampering, collusions, slandering, overstating and etc. Thus, such threats need to be mitigated to help traders to establish sufficient trust among themselves to give them confidence to participate in ad hoc m-commerce trading systems.

Mobile device's physical security which might be compromised or the device itself stolen by criminals and thieves. Compromised devices could allow attackers to exercise the owner's privileges and get direct access to all resources available on those devices. On the other hand, loss of mobile devices might prevent their owners from being able to get necessary information about their transactions, which could subsequently lead to incomplete transactions and lost opportunities to trade.

Application code which might be modified or tampered with, as ad hoc m-commerce applications could well be implemented on open-source developer sites. Thus, it is important to ensure that the traders use a legitimate ad hoc m-commerce application from the beginning and get its valid updates in a reasonably timely way.

3.3.2.2 Possible Threats

There are many possible threats to an ad hoc m-commerce trading system, which can exist in a variety of ways. However, with respect to the security objectives of an ad hoc m-commerce trading system, this thesis only focuses on the most relevant

threats in such a trading system. To keep the list of identified threats restricted to only the most relevant threats in an ad hoc m-commerce trading system, it is assumed that:

- Traders obtain ad hoc m-commerce applications and their updates, which might be developed on open source community development lines from a trusted source or recognized outlet.
- Traders maintain the physical security of their mobile device and its local repository.
- Hard to defend against attacks on network communications such as traffic analysis and jamming attacks are likely to be a rare occurrence.

Thus, threats arising in relation to the physical security of mobile devices or the perversion of the code of ad hoc m-commerce specific applications or platforms will be out of the scope of this thesis. Under these provisos the most salient threats that exist within an ad hoc m-commerce trading system are:

Spoofing - Whenever traders in an ad hoc m-commerce trading system communicate with each other through an insecure ad hoc wireless network communication channel, there is a threat of spoofing identity or authorship. Targets for spoofing are the online identity of the traders and integrity or authorship of messages being exchanged among them.

Tampering - Tampering can be done while data is on the communication channel or while data resides on traders' mobile devices. Targets for tampering are the identity credentials in a digital certificate, reputation reports, membership data, transaction contracts, testimonials and so on.

Unchallengeable Repudiation - Repudiation can occur whenever any trader denies that he has performed a specific action or transaction that it seems he has done but evidence is lacking to prove otherwise. It matters when such repudiation risks loss to another party but the target of the action has no way to demonstrate that the repudiator is not being truthful.

Information Disclosure - Information can be leaked during communication or while being stored on traders' mobile devices. Similar to tampering threats, targets for information disclosure are the identity credentials, reputation reports, membership data, transaction contracts, testimonials and so on.

Collusion - Collusion can occur whenever two or more traders conspire to perform specific actions in order to cause unfair damage to other parties' reputation or reasonable trading prospects.

3.3.3 Types of Threats

Based on the discussion and assumptions made in Section 3.3.2 above , assets within an ad hoc m-commerce trading system can be viewed from three different aspects; traders' online identity, data or information stored on their mobile devices or being exchanged among them and also their reputation which is influenced by their behaviour in performing transactions and other related activities within the trading community. Each of these aspects poses threats to the trading system, and thus, in this thesis, the threats are categorized as follows:

3.3.3.1 Identity-related Threat

Traders in ad hoc m-commerce trading systems are represented by their online identity via their trading pseudonym. Using pseudonyms to participate in online transactions in such a loose ad hoc community exposes them to security attacks such as identity spoofing, Sybil attacks and also whitewashing.

Identity spoofing (masquerade) - Identity spoofing is where an ill intentioned trader tries to pass himself off as someone else. The prime risk is that he may use that spoofed identity to defraud other traders. Possible scenarios of identity spoofing in ad hoc m-commerce trading systems include the following:-

- An ill-intentioned trading party uses the trading pseudonym of a reputable trading party in order to claim the reputation of that trading party to induce other traders to transact with him and then defrauds them. In doing this, the reputation of that reputable trading party is likely to be damaged.
- An ill-intentioned trading party uses an honest trading party's trading pseudonym to disguise their role in attesting ill-intentioned associates' false identities, reputation reports, membership data and so on.

Sybil Attacks - Sybil attack is where an ill intentioned trader creates multiple trading pseudonyms to cheat collective decision making processes and aggregations of multiple people's judgments to subvert the trading system. In ad hoc m-commerce trading systems, an ill-intentioned trading party may use multiple identities to do the following:-

- To create bogus transactions with some of these identities and then publish ill-founded positive evaluations of those transactions with others of them in order to increase these identities' reputations.
- To collude to give unfair negative evaluations to an honest trading party in order to damage that party's reputation.

- To manipulate the attestation process for example to attest false identities or membership data or support unfounded reputation reports of his ill-intentioned associates.

Whitewashing - A whitewasher is a trader that leaves a particular trading forum and then re-enters with a new identity to hide his bad reputation or misbehaviour. In ad hoc m-commerce trading systems, a trading party may use whitewashing to escape his bad reputation recorded in previous deal evaluations.

3.3.3.2 Information-related Threat

As communications and activities related to the exchange of information in ad hoc m-commerce trading systems are conducted solely over an insecure ad hoc wireless network and may involve routing via intermediary peers, participating parties in such trading systems are vulnerable to man-in-the-middle attacks. Information or data stored on traders' mobile devices is also subject to tampering and disclosure to unauthorised parties. The owner or a third party might attempt to tamper with the data or disclose it without permission. The tampering might be achieved by simply editing the data or adding more data or deleting some parts of the data or the whole data either where it is stored or while it is in transit.

Man-in-the-middle-attacks - A man-in-the-middle attack is where an ill intentioned trading party covertly intercepts communications between two parties. The ill intentioned trading party can then control the communication and tamper with or omit messages being transferred without the knowledge of either the original sender or the recipient of his intervention. Some possible scenarios of man-in-the-middle attacks in ad hoc m-commerce trading systems include the following:

- An ill intentioned trading party intercepts communications between two parties who exchange their deal evaluations after the completion of a transaction and alters the deal evaluations without their knowledge.
- Trading parties that act as intermediaries manipulate information that is being transferred via them to other parties. For example, an intermediary peer discards a propagated unfavorable deal evaluation that is being transmitted via his node without being detected by the two end parties.

3.3.3.3 Misbehaviour-related Threat

With dynamic participations in an ad hoc m-commerce trading forum [118], it is to be expected that traders will often engage in a transaction with parties that they do not have any prior experience of or have never met before. This will make them susceptible to subversive behaviour by their trading counterparties, such as being

given misleading trade descriptions or unfair deal evaluations or being subject to repudiation misbehaviour and collusions.

Trade Misdescriptions - An ill-intentioned trader may cheat other members of a trading forum by offering fake items as real or by trading items that are not as described in the offer.

Unfair Deal Evaluations - In ad hoc m-commerce trading systems, traders might be expected to evaluate each other after the completion of each transaction by generating a deal evaluation. Infrastructure supported trading systems over the Internet like eBay have established this as a norm. This deal evaluation can be used to assess each trader's reputation. If a transaction concludes positively, traders would be expected to express their satisfaction about the transaction in their deal evaluations, digitally sign them and then send them to their trading counterparts. Otherwise, they can share their bad evaluation of their trading counterpart with other traders in the trading forum to make them aware of that party's negative behavior. However, an ill-intentioned trader may manipulate the reputation of other traders by giving unfair evaluations of transactions. There are at least two types of unfair evaluations; overstating (unfair positive) and slandering (unfair negative). Overstating is where a trader inaccurately evaluates a bad or mediocre transaction as good. This may be poor judgment or done to boost the reputation of an associate. Slandering is where a trader inaccurately gives a negative evaluation to a good transaction. Again this may be poor judgment or done maliciously to lower the reputation of a reputable trader.

Repudiation Misbehaviour - Repudiation misbehaviour occurs when a trader performs a particular action and then denies having performed it. There are at least two significant types of repudiation misbehaviour; data repudiation and contract repudiation. Data repudiation occurs when a trader sends a particular message or document and then denies having sent that message or document. For example, an ill-intentioned trading party sends a bogus transaction contract without digitally signing it and then denies having sent that contract. In this case, its trading counterparty will not be able to prove that the contract has been sent by that ill-intentioned trading party. Contract repudiation occurs in a situation where one party initiates a transaction or has agreed on a transaction contract and then denies having initiated the transaction or having agreed on the contract.

Collusions - Collusion is where multiple ill-intentioned traders conspire to influence their own reputation or other traders' reputation, group decision making processes, attestation processes and so on. For a reputation system, there are at least two types of collusions; hyping and bad mouthing. In hyping, a trader colludes with associates to give inauthentically good evaluations or testimonials to increase his reputation

beyond what it should be. He can then try to use his bogus good reputation for fraudulent purposes. Bad mouthing is where a group of traders conspire to harm the good reputation of a trader by each giving unfair negative evaluations to that trader.

3.3.4 Possible Countermeasures

Similar to infrastructure-based networks, one of the most common security mechanisms that can be used to protect traders of ad hoc m-commerce against security attacks aimed at identity disguise is public key cryptography. It provides a variety of techniques for online identification, including use of digital certificates. It also can be used to protect traders' data or messages from being tampered or disclosed, using digital signatures and encryption.

For misbehaviour-related threats, one way to mitigate those threats is by having a means to establish trust among traders. A reputation system can be an effective means to do this as it provides a collaborative method for traders to assess the trustworthiness as well as predict the future behavior of other traders based on sharing their past trading history and testimonials of tradeworthiness. In addition to that, it helps traders choose reputable parties to trade with and avoid dealing with dubious ones.

A third effective measure that is widely used in trading communities is to restrict trading to recognized parties in good standing and to put in place a validation scheme to control admission to only those who can be adequately vouched for and to exclude those who are recognized by other members as not behaving properly.

All three measures rely on some trading parties attesting, vouching for or approving the behaviour of other parties. These relationships are also themselves a useful resource in mapping patterns of association among parties.

3.3.4.1 Public Key Cryptography

Public key cryptography provides a means for establishing secure communication between two parties over a nonsecure communication channel. It can be used to provide security services for data authenticity, integrity, confidentiality, and non-repudiation, as well as identity authentication. This cryptographic approach uses two different keys and employs asymmetric key algorithms [47]. One of these keys is kept private and the other is published or made publicly available. These algorithms can be used not only for encryption of messages, but also to implement digital signature schemes. Encryption of messages will ensure that messages or documents sent across the network are unreadable by any third parties other than the authorized

recipients, such as eavesdroppers or peers that act as intermediaries. Messages can be encrypted with the public key of the recipient and/or signed by the private key of the sender and then decrypted with the other key. Digital signatures ensure the authenticity, integrity, and non-repudiation of the data transmitted over the communication channel.

Digital Signatures - A digital signature is an electronic signature that functions like a traditional handwritten signature in many aspects. It is created when a digest of the message or document to be transmitted is enciphered using a private key. The use of a private key to encipher the digest of the message or document helps to authenticate the identity of the sender of the message or document, as it could only have been enciphered using the private key of the sender. The recipients can verify the signature by deciphering it using the public key of the sender. This will ensure that the sender of the message or document cannot credibly deny having signed or sent the message or document. A digitally signed document or message is also unalterable by third parties after the signature without this being detectable, which will give assurance to the recipients that the original content of the transmitted message or document was not altered in transit. Digital signatures are based on digital certificates.

Digital Certificates - A digital certificate is an electronic document that provides a testable warrant that the public key in it is the public key of the identity enclosed within it. It furnishes a means to establish the identity of an individual or organisation in online environments, particularly in electronic transactions [168]. It uses digital signatures by third parties to bind the public key of the certificate owner to his identity information such as name, address and so on. A digital certificate normally contains at least the following information:

- A public key of the owner
- Identity Information such as owner's name or alias or pseudonym, address and so on.
- Expiration date of the certificate
- One or more digital signatures of its issuers

In the case of electronic transactions, digital certificates together with encryption provide a security solution to assuring the identity of all parties involved in a transaction. A digital certificate makes it possible for the participating parties to verify the identity of the party that they are dealing with is whom he or she claim to be and thus, prevents others from impersonating that particular identity.

However, to guarantee the validity of the information in the certificate, it needs to be issued and signed by independent and recognized trusted third parties that warrant its validity. Relying parties can check on that warrant by verifying the digital signature of the certificate's issuer, which can only have been created using that issuer's private key. The degree of confidence in the validity of the certificate will depend on the level of trust that the relying parties have in its issuers. There are two approaches commonly used to get this trust. One approach is typically used in a public key infrastructure (PKI) scheme [38],[145],[143], where the certificates are issued and signed by an authority, referred to as a certification authority (CA). Another approach is the web of trust scheme [184],[185] that uses certificates signed by multiple parties.

PKI Scheme - In the PKI scheme, the CA is a primary component that functions as a trusted third party that manages the digital certificate life cycle, from issuance through revocation or suspension of certificates until their expiry. The CA is trusted by both the owners of certificates and the parties that rely upon the certificates. A CA is a person, department, company or other organisation that issues digital certificates to its users. CAs can either be public and commercial or private. Public commercial CAs such as VeriSign, Entrust and DigiCert are often trusted by a large number of users and charge their users subscription fees in order to issue certificates. Private CAs are normally operated by large organizations or government entities for their internal usage. There are also some network service providers that act as a CA issuing digital certificates to their subscribers at no cost. To enable the relying parties to obtain other users' certificates, the CA may post the certificates that it has issued to a central repository which is available online and accessible to the relying parties.

In a PKI scheme, users are required to provide some personal information that will verify their identity in order to request a digital certificate from the CA. Some CAs may only require users to provide a little information, such as their real name, home address and e-mail address. Others may require more information and stricter proof of that identifying information such as a passport, birth certificate, driving licence, bank statement and so on before issuing a certificate.

The users of PKI will accept the identity credentials in a digital certificate as valid if they trust the CA to have verified the identity and public key as belonging together and can verify the CA's signature. They place their trust in the CA based on several trust models, which include the following:

1) Single CA Model - This is the most basic model where there is only one CA that provides PKI services like issuing, signing and revoking digital certificates and so on [138], as shown in Figure 3.1. Each certification path starts with the public key of this CA only.

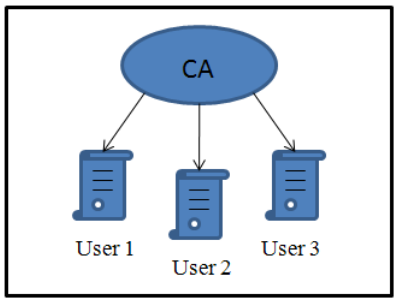


Figure 3.1: Single CA Model

2) Hierarchical Model - In this model, there is more than one CA, where the most trustworthy CA will be the root CA (RCA) [138], as shown in Figure 3.2. The trust relationship is specified in only one direction where the RCA only issues certificates to its subordinate CAs and those CAs may then issue certificates to their subordinate CAs or users and so on. The certification path starts with the RCA's public key and thus, all users need to know the public key of the RCA.

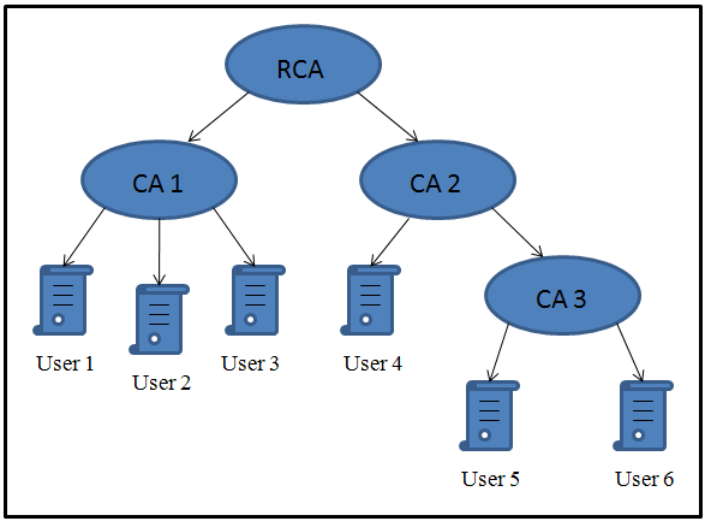


Figure 3.2: Hierarchical Model

3) Mesh Model - This model is also known as a crosscertificate architecture [99],[138]. In this model, all the CAs are independent and any CA can perform peer-to-peer cross certification with other CAs as shown in Figure 3.3 [138], except if there is any constraint or limitation specified in the certificates. Users may choose to trust any CA in the architecture but the trust anchor of a user will be its local CA. The certification path begins with the local CA certificate.

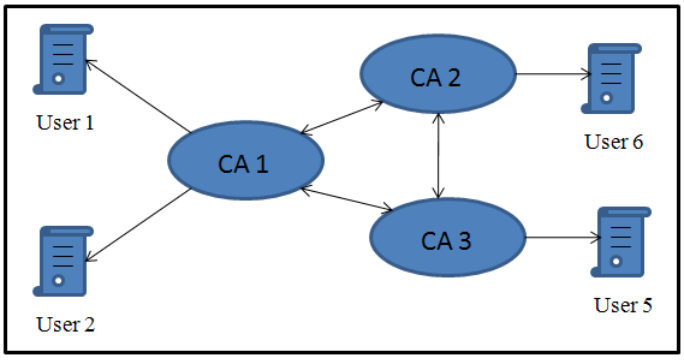


Figure 3.3: Mesh Model

4) Bridge CA Model - This model is based on a central CA that acts as a hub or bridge to cross-certify with other CAs [38], as shown in Figure 3.4. It combines the concepts of both the root CA and crosscertificate. Polk and Hastings in [125] use this model to establish a peer-to-peer trust relationship among various communities of users.

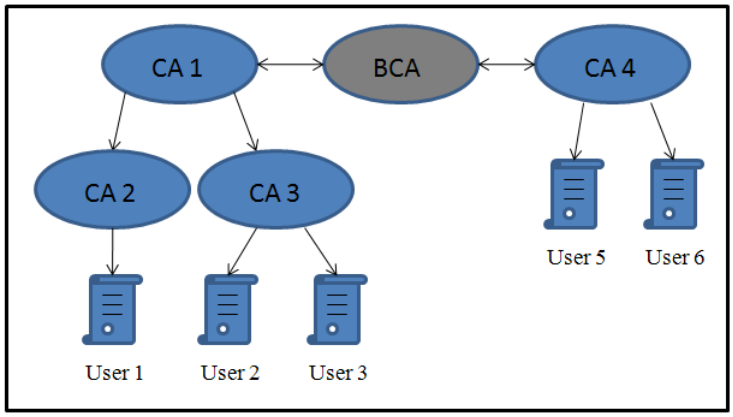


Figure 3.4: Bridge Model

However, although a PKI scheme enables secure, reliable and efficient digital certificate and key management facilities, it does not seem to be suitable for deployment with ad hoc m-commerce. This is because this kind of scheme requires a pre-established network infrastructure for communications between the users and CAs, which is unlikely to happen in ad hoc wireless networks because it is infrastructure-less. In addition to that, the dynamic topology of ad hoc wireless networks makes it impossible for the users of an ad hoc m-commerce trading system to rely on a communal CA to provide such services, such as in the single CA model, or in the hierarchical model that relies on a RCA. Topology changes in the network may result in frequent network disconnections, which subsequently may cause the CA to be unavailable to provide required services such as checking a certificate's revocation status.

Furthermore, it seems unlikely that traders in an ad hoc m-commerce trading system would be willing to pay any subscription fee in order to obtain a digital certificate from a well recognized CA such as Verisign just to participate in informal and low value trading. Although there are some network service providers that provide CA services for free, none of them can be relied upon to provide such services to ad hoc m-commerce traders due to the infrastructure-less nature of an ad hoc wireless network. Traders in an ad hoc m-commerce trading system may also not want to go through the bother of having to supply their personal information to the CA and satisfy some background checks just to obtain a digital certificate to participate in such informal and low value trading.

It also cannot be expected that all participating parties of an ad hoc m-commerce trading system will obtain their digital certificates from the same CA. This can be an issue as relying parties may have difficulties or may not be able to verify the digital signature on a certificate issued by a different CA. Another issue with a CA is that if the CA's private key is compromised, then the security of the entire system is lost for each user whose certificate is issued by the CA. This will require re-issuance of some or all of the previously issued certificates in the system.

From the discussion above, it seems that a PKI scheme is not suitable for an ad hoc m-commerce trading system due to its characteristics and the infrastructure-less nature of an ad hoc wireless network. Ad hoc m-commerce requires a scheme that is self-organized, P2P, where the function of a trusted signer of certificates is distributed over all users [183] and involves no cost.

Web of Trust Scheme - A web of trust is a concept used in Pretty Good Privacy (PGP), which was first introduced by Phil Zimmermann in [184],[185]. Abdul Rahman [7] then used this concept in his PGP Trust Model. In this scheme, there is no central authority that can be relied upon to provide digital certificates or key management facilities. Certificates are issued by the users themselves. Any users in the network can act as a certifying authority that signs and validates other users certificates. These signatures gradually form a set of interconnected associations of individual public keys or "Web of Trust" as shown in Figure 3.5.

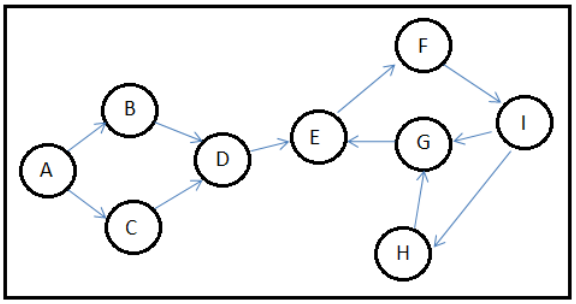


Figure 3.5: A Web of Trust Model

The users of this scheme place their trust in the certificate's issuer and attestors based on their personal experience or knowledge or recommendations by other known and trusted parties. Such trust in other party's signature to attest a PGP certifcate is placed based on the following three levels of trust:

- Complete trust: A user is fully trusted to validate others' public key and identity credentials binding.
- Marginal trust: A user is marginally trusted to validate others' public key and identity credentials binding.
- No trust (or Untrusted): A user is not trusted to validate others' public key and identity credentials binding.

The validity of the PGP certificates will only be accepted if the relying party recognizes one or more parties who have attested relevant certificates as trusted parties. A PGP certificate is considered as valid if it is signed by one fully trusted party or two marginally trusted parties.

This scheme seems to be suitable for deployment in ad hoc m-commerce due to its dynamic, P2P and distributed characteristics [48]. However, its normal incarnation on the Internet requires a public certificate directory to store and distribute certificates, which is usually located at an online and centralized trusted third party entity. This online and centralized public certificate directory is impractical to require in ad hoc m-commerce as the availability of the trusted third party where the directory is placed cannot be guaranteed all the time due to frequent network disconnections as well as irregular participation by trading parties. To enable this scheme to be used in ad hoc m-commerce, storage of certificates needs to be decentralized and some effective decentralized scheme for certificate revocation needs to be devised. In addition to that, due to infrequent communications among traders in ad hoc m-commerce, there needs to be an appropriate attestation mechanism to vouch for the continuing validity of the certificates in such a loose community.

3.3.4.2 Reputation System

Reputation Systems are essentially feedback systems which enable participating parties in a transaction to provide feedback on each other [134]. The feedback usually consists of a rating (positive, neutral or negative) and comments, and these ratings and comments can be aggregated to represent the reputation of a user in the system. The original design goals of reputation systems are to assist users in deciding who to trust in a system, to encourage trustworthy behaviour, and to discourage and deter untrustworthy or dishonest people from participating in the system where the reputation system is implemented [134].

Reputation systems have already proven useful in many commercial online applications. In eBay's reputation system [1], a buyer can rate a seller by giving a positive, negative or neutral rating and also a short comment after the completion of each transaction. An overall score is computed based on the percentage of the total number of positive and negative ratings that a seller has received for the past 12 months. A buyer can also provide more detailed information about a seller by giving a 5-star rating on the aspects of the item's description, communication, delivery time and postage and packaging charges. An average rating for each aspect is published. A study by [134] shows that eBay ratings encourage users to engage in transactions offered by highly rated sellers and sometimes allow them to charge higher prices.

3.3.5 Possible Vulnerabilities

Vulnerabilities are security weaknesses that can be exploited to make a system susceptible to an attack [116]. Similar to other systems, an ad hoc m-commerce trading system could also be vulnerable to attacks if its security services are not implemented in a proper manner, especially in utilizing public key cryptography for the establishment of its traders' online identity and also data encryption and authentication. In order to prevent ill-intentioned parties from compromising the security of an ad hoc m-commerce trading system, locating and mitigating vulnerabilities in the design phase of its security services is a critical step.

Thus, according to the key assets of the trading system as discussed in Section 3.3.2.1, this thesis classifies possible vulnerabilities in an ad hoc m-commerce trading system to the following:

3.3.5.1 Vulnerabilities Associated with Digital Identity

Due to the dynamic and infrastructure-less nature of an ad hoc wireless network, the implementation of public key cryptography in an ad hoc m-commerce trading system requires careful consideration and needs to be done properly. Improper implementation can create several vulnerabilities that are associated with traders' digital identity, data and so on.

Common public key cryptography's vulnerabilities associated with traders' digital identity include the following:

Weak digital certificates' verification process - This is due to lack of processes to verify the identity credentials in a trader's digital certificate when they create their online identity, which will make it easier for ill-intentioned trading parties to spoof another party's identity, create multiple identities or re-enter the trading system with a new identity. This problem is likely to affect honest trading parties who

might be defrauded and also reputable trading parties whose reputation might be damaged when the false identities are taken as legitimate.

Weak, stolen or compromised cryptography keys - One of the implications of this vulnerability is that ill-intentioned parties can use weak, stolen or compromised cryptography keys to spoof another party's identity or produce a valid digital signature to attest fake certificates, trading histories or membership data of their associates. A digital certificate whose corresponding private key is stolen or compromised needs to be revoked. New key pairs need to be generated and a notification about the certificate revocation needs to be distributed to all participating parties of the trading system. It may take considerable time to notify all participating parties, especially in such a dynamic trading system.

Long-lived digital certificates - Digital certificates are normally valid for a year or more [54]. Certificates that have a long validity period, for example 5 years or more, may contain attributes that cease to be valid during the time it is nominally current. An old photograph in a certificate may have ceased to look the same as the current physical appearance of its owner. This might cause the other parties in the trading system to consider the certificate as no longer valid as the validity of the photograph, which is part of the identity credentials in that certificate, cannot be verified. Another issue with a long-lived digital certificate is that its corresponding private key is vulnerable to being accidentally disclosed or compromised, as the time during which it might become available to an attacker will be considerable.

3.3.5.2 Vulnerabilities Associated with Data

Another potential security vulnerability in utilizing public key cryptography is the possibility of a man-in-the-middle attack, which could occur due to the following:

Unencrypted communications - This may arise from wilful disregard of security procedures of the trading system or as a normal action taken in spontaneous circumstances. This might enable the eavesdroppers who monitor the network to reveal or tamper with the unencrypted data.

Unsigned messages or documents - This may arise from wilful disregard of procedures of the trading system to digitally sign any messages or documents before sending them over the network or as a normal action taken in spontaneous circumstances. The implications of this kind of vulnerability is that the authenticity and integrity of the messages or documents being sent cannot be assured and this will enable the ill-intentioned parties to credibly deny sending those messages or documents.

Stolen or Compromised private keys - This will enable the ill-intentioned parties to use the compromised private key to tamper with the data being transmitted

between two parties without the knowledge of the two end parties. In addition to that, with the stolen or compromised private key, the ill-intentioned parties can send messages using that private key or produce a perfect digital signature to sign messages or documents in the name of the party whose private key is compromised.

Bogus public keys - In public key cryptography, users' public keys should be made publicly available so that other users can use those keys to communicate and exchange information with the key owners securely. One of the significant issues of public key cryptography is that users must be able to trust that a public key really belongs to the person to whom it purports to belong. It is important for users to be aware of this kind of vulnerability as they may become a victim for trusting the public key presented by an impersonator. This is because they may unintentionally disclose confidential information to the impersonator when they send a message or document that is encrypted using the bogus public key, which will then allow the impersonator to decrypt and read the contents of the confidential message or document with its corresponding private key.

3.3.5.3 Vulnerabilities Associated with Reputation System

In addition to the above vulnerabilities, inappropriate implementation of public key cryptography could create other vulnerabilities associated with the reputation system in an ad hoc m-commerce trading system. This is due to the fact that such reputation system is highly dependent on a valid identity of a trader and also the authenticity, integrity and non-repudiation of the messages or documents being exchanged among traders. The reputation system itself provides opportunities for ill-intentioned traders to collude in order to gain unwarranted benefits from the system.

3.4 Security Requirements for Ad Hoc M-Commerce Trading Systems

To create sufficient confidence among traders to engage in ad hoc m-commerce transactions and its other related activities, the identified threats and vulnerabilities above need to be addressed or mitigated to an acceptable level. It seems that the design of its security services requires careful considerations on the following aspects:

3.4.1 Constraining Participation

One of the major security concerns in ad hoc m-commerce trading systems is to establish sufficient trust among its participating parties in order to mitigate the uncertainty and risks involved in its transactions. As mentioned in Section 3.3.4 above, a reputation system can be an effective means to develop such trust among traders in an ad hoc m-commerce trading system. However, a reputation system alone cannot guarantee that all participating parties in such trading systems will behave properly and remain trustworthy all the time. Some traders may carry out each of their transactions honestly while some others may only carry out certain transactions honestly but deceive when engaging in other transactions. Thus, it is important to restrict an ad hoc m-commerce trading system participation to only parties regarded as reasonably trustworthy by other participating parties of the trading system. This can be achieved using group membership to set acceptable limits of behaviour for traders and to specify how collective decisions are to be obtained. It can be the first step towards creating an environment that is secure to some degree for traders to communicate and collaborate with each other, as well as to engage in online trading. More detailed discussion about an ad hoc m-commerce trading system's group membership will be presented in Chapter 7.

In order for the group membership management in an ad hoc m-commerce trading system to function in an effective manner, it requires a reliable online identity support scheme. This is because a trader's identity-membership information binding will help traders to determine the validity of each membership claim by their peers online. It also enables traders to verify the authenticity, integrity and non-repudiation of messages or documents being exchanged among traders in collaborative decision making processes for group membership management.

3.4.2 Sharing Trading Experience

In an ad hoc m-commerce trading system, it is important for traders to share their trading experience, either positive or negative with other traders to help them make trust decisions. Traders can share positive experience of their trading counterparts in their recent trading histories with other potential trading partners in order to provide evidence of those counterparts' good faith. Traders can also share their negative experience about a particular trader with other members of the trading system to make it harder for that trader to behave dishonestly in future transactions. However, the sharing of such trading experience may cause traders to make inaccurate decisions in choosing the right party to trade with if the availability, integrity and reliability of such information cannot be assured, as it might not be available when

it is required or might be tampered during transmission or be manipulated by ill-intentioned parties for their own benefits.

Thus, an appropriate mechanism is required to enable traders to verify the authenticity, integrity and non-repudiation of such important information as well as to ensure its availability, reliability and efficient retrieval. In addition to that, the identity of the party who is providing the information also need to be verified to ensure that it comes from a trusted party.

3.4.3 Sharing Expressions of Trust

Trust is vital in an ad hoc m-commerce trading system and it can be generated through relationships among traders. As such relationships develop, traders will gain more information about each other through their experiences, which will then establish some degree of trust among themselves. However, in such a loose and dynamic ad hoc m-commerce trading community, it cannot be assumed that all traders know each other and have established trust relationships among themselves. There are likely to be traders that irregularly participate in the trading system's activities and also new traders will replace traders that drop out. These kind of traders may not have sufficient information about their potential trading partners or other traders in the trading community to establish a satisfactory level of trust among themselves. Thus, it is important for the traders to share their expressions of trust about any particular trader that they know well with other traders to help new and infrequent traders determine the extent to which they can trust other traders. For instance, if several other traders trust that a particular trader's identity credentials in a digital certificate are genuine, then a possible trading partner is likely to assume those credentials are genuine as well and use them to determine to what extent to trust that identity if those other traders seem reputable themselves.

However, similar to the sharing of trading experience, the sharing of such kind of trust information requires traders to be able to verify the authenticity and integrity of the shared information, as well as the identity of the traders who are providing the information.

3.5 Conclusion

In order to find appropriate security solutions for an ad hoc m-commerce trading system, this chapter defines a threat model that help specify the security objectives and key assets of the trading system. The threat model also identifies a set of possible

threats that could subvert the functionality of such trading system. The threats are classified into three main categories; namely identity-related threats, information-related threats and misbehaviour-related threats. The threat model also makes recommendations on possible countermeasures for each category of the threats and identifies several vulnerabilities that can be exploited by an ill-intentioned party in an attempt to compromise the security of the trading system, if the countermeasures are not properly designed and implemented.

To mitigate the identified threats and vulnerabilities, the design of ad hoc m-commerce security services needs to consider carefully three main aspects; constraining participation in the trading system, sharing trading experience and sharing expressions of trust among traders. The suggested countermeasures in Section 3.3.4 need to be modified and implemented in a way that can suit with the nature, characteristics and security requirements of an ad hoc m-commerce trading system.

Chapter 4

An Ad Hoc M-Commerce Trading System Framework

4.1 Introduction

This chapter presents the design of an ad hoc m-commerce trading system, a framework for m-commerce trading conducted online and wirelessly outside established computer infrastructures. This framework provides a foundation structure for application developers to organize the effective development, maintenance and enhancement of such trading systems. It takes into consideration the general capabilities and also constraints of mobile devices without specifying any device platform or operating system in particular, so that application developers can focus on the design and implementation of certain aspects or services that are required to support the core functionality of the trading system. In this thesis, this framework serves as a basis for addressing the major security issues involved in trading wirelessly among computing nodes in a dynamic network and in the absence of a network service provider, as discussed in Chapter 3.

Section 4.2 gives the general idea of how an ad hoc m-commerce trading system operates and discusses the processes that need to be performed by a trader in order to join a particular trading system. This section also discusses the activities that traders are allowed to perform when they participate as a member of a particular trading forum. Section 4.3 presents the abstract architecture for an ad hoc m-commerce trading peer and further explains the functionality of each of the services provided by the service layer. Section 4.4 discusses the four main steps involved in an ad hoc m-commerce transaction. As the main objective of this thesis is to define an environment that is sufficiently secure for traders to participate in ad hoc m-commerce transactions, Section 4.5 further elaborates on the design of an ad hoc

m-commerce trading system framework membership service and also its security and trust service. Section 4.6 discusses the key characteristics of the ad hoc m-commerce trading system framework. Section 4.7 compares the design of an ad hoc m-commerce trading system framework with existing infrastructure-supported m-commerce architectures and examines their characteristics and discusses several fundamental differences between their characteristics and implementation. Finally, Section 4.8 concludes this chapter.

4.2 Ad Hoc M-Commerce Trading System Overview

An ad hoc m-commerce trading system is a platform for mobile users to engage in mobile commerce transactions using ad hoc wireless networking. It is a self-organized and self-configured m-commerce venue that can be initiated anywhere by any two or more traders that are in close proximity with each other and does not require any third party infrastructure to support it. To participate in the trading system, traders must be equipped with a Wi-Fi capable mobile device and an appropriate ad hoc m-commerce application. Traders can join the trading system as a seller or buyer or both. The trading system does not limit its participating parties to engage in ad hoc m-commerce transactions only, but it allows the traders to communicate and collaborate with each other to control and manage its group membership management and security and trust service which include the following:

- Give recommendations about other traders' online identities, trading histories, testimonials and reputations.
- Attest other traders' digital certificates that bind together their identity information with their public keys, membership information, testimonials and trading histories.
- Evaluate each other after each transaction by providing deal evaluations. The deal evaluations are used by the traders as a means to express their satisfaction about their trading counterparts' behaviour in fulfilling their transaction agreements.
- Share negative evaluations about their trading partners with other traders in the forum.
- Sanction those traders who misbehave or have a history of being given poor evaluations.

Each trading system will operate a trading model such as for swapping of digital resources or selling or buying items or for conducting online auctions and so on, and

have policies governing how it handles dissemination of trust data and deals with forum membership and sanctions. Some forums will have an open membership while others will have a closed membership or be open to all but banned parties. More details about a trading system's group membership will be discussed in Chapter 7.

To join a trading forum, traders must first activate the appropriate m-commerce application on their mobile device and create an online identity to represent themselves in the trading system. More details about a trader's online identity establishment will be presented in Chapter 5. Prospective traders are expected to send a join request together with their identity credentials to any available peers that are within communication range with them. Once accepted as a member of a particular trading forum, traders can engage in m-commerce transactions, as well as participate in any of the trading system's activities as mentioned above.

4.3 The Abstract Architecture

As this thesis focuses on the use of mobile devices that operate as peers with a similar role to each other in a dynamic and decentralized network, the design and implementation of an ad hoc m-commerce trading system is based on a P2P architecture. Figure 4.1 below illustrates the abstract architecture for an ad hoc m-commerce trading peer.

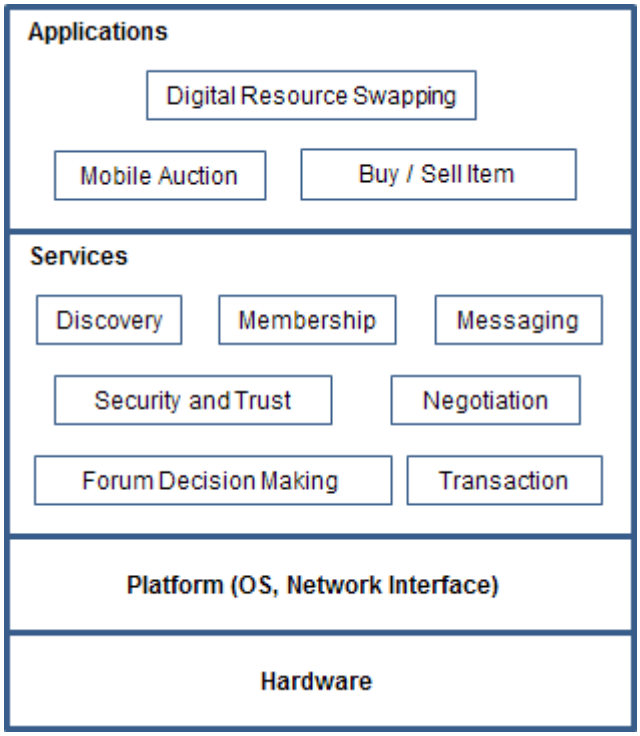


Figure 4.1: An abstract architecture for an ad hoc m-commerce trading peer

The first two layers sequentially include a mobile device and an operating system required for operating the m-commerce applications. The Service layer provides services that are required to support the core functionality of the trading system which include the following:

Discovery Service - Provides the ability for peers to search and discover available trading forums, advertisements and other peers in the network. For a mobile host to join a group, or for a group to merge with another group, they must be able to find out what groups are present in their vicinity. The discovery protocol carries out this function and serves as a supporting layer for the group membership maintenance protocol.

Membership Service - Provides the ability for peers to organize themselves into a trading forum, which includes the ability to join, renew membership and also to exclude a member from a trading forum.

Forum Decision Making Service - To facilitate any forum wide decision making processes by fostering effective communication among forum members.

Messaging Service - Provides support for message delivery over the network. This includes specifications for routing, relaying and propagating messages as well as the message structure and so on.

Security and Trust Services - Provides support for identity establishment, trust establishment as well as message authentication, integrity, confidentiality and non-repudiation. This service will also provide security advice to make participating users understand the issues and their responsibilities in securing ad hoc m-commerce trading systems.

- Message authentication and encryption in order to ensure the authenticity, integrity and confidentiality of the messages transmitted over the network.
- Peer authentication to ensure that communications are with valid peers. When a trader joins a trading forum, he has to provide his digital certificate that consists of his trading pseudonym, photograph and digital signature as his identity credentials. The digital certificate needs to be digitally signed by at least one other party that is considered as a trusted party by other peers to confirm its validity.
- Identity establishment which includes generating public and private key pairs, signing PGP certificates as well as verifying the certificates.

Negotiation Service - To facilitate a negotiation process during a deal until a mutual agreement or disagreement is reached between the participating parties.

Transaction Service - To facilitate the processes for traders to complete a transaction, which may include a payment process.

The Application layer is the implementation of ad hoc m-commerce applications such as mobile auctions, swapping of digital resources, buying or selling items and so on.

4.4 The Standard Trading Pattern

To participate in ad hoc m-commerce transactions, traders must first join a trading forum that offers services that they are interested in such as to buy and sell second hand goods. It is expected that after a party advertises items to be traded and potential trading parties express their interest, traders will perform transactions according to at least the following four main steps, as shown in Figure 4.2.

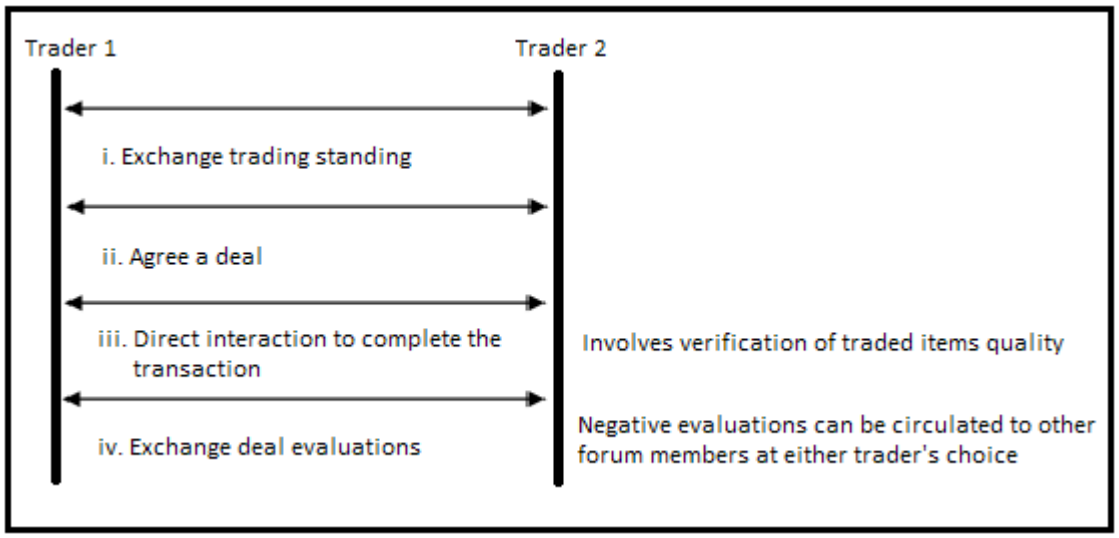


Figure 4.2: Four main steps involved in an ad hoc m-commerce transaction

Exchanging trading standing - In this step, both traders will exchange their digitally signed trading standings which consist of a set of recent deal evaluations and any testimonials that they have as well as their membership voucher and PGP certificate. Each will check the PGP certificate [119] and membership voucher [118] offered as satisfactory. The PGP certificate can be checked through the certificate authentication process, which will be discussed later in Chapter 5, while membership voucher can be checked through the membership voucher verification process, which will be discussed in Chapter 7.

After evaluating each others' reputation and checking their local repository to see if any negative reputation report or forum exclusion proposal has been made against the other party as well as considering the potential risk involved in the transaction,

both traders will decide whether or not to enter into a transaction. A trader may receive responses from more than one potential trading partner. In this case, a trader needs to decide with whom to trade with after assessing the trustworthiness of potential trading counterparties and considering the potential transaction risks.

Agree a deal - The traders will negotiate a deal based on the advertised trade. It will specify the terms including what is to be exchanged for what and how this will be effected. If both of the traders agree with the deal and decide to proceed with the transaction, the process will continue with both parties digitally signing a transaction contract which is produced by instantiating it from a standard pattern approved by the forum. The transaction contract will consist of at least the following information; both traders trading pseudonyms, items to be exchanged or purchased (i.e., name, type, specifications of the items), quantity, price per item, delivery date and place, method and date of payment, digital signature of both traders, time and date the contract is signed.

If no deal is finally agreed between the traders, then the transaction will not take place. The trader who initiates the transaction may prefer to try to make a deal with another potential trading partner instead.

Direct interaction to complete transaction - At this stage, if no party repudiates the contract, the transaction will take place where both traders will interact directly to try to complete the transaction. This will involve a step of verification during which each party will assess whether the offered resource or item is as described or whether the money or swap offered is as agreed. The identities of the parties will also be further verified by checking that the photograph on the other trader's PGP certificate resembles his current appearance [119] (in the case that both parties did not have a physical meeting during the authentication process of their digital certificates).

If one of the traders repudiates the contract, then his trading counterpart may call off their deal. In this case, although the transaction between the traders does not take place, the trading counterpart may circulate a negative evaluation about that trader's misbehaviour for repudiating their transaction contract in the trading forum.

If one of the traders calls off the deal, his trading counterpart may also circulate an adverse evaluation about that trader's misbehaviour for breaching their transaction contract in the trading forum.

Exchange deal evaluations - After the completion of each transaction, traders are expected to generate a deal evaluation about the trade, digitally sign it and then send it to their trading counterparty. The deal evaluation will also contain

the transaction contract that is digitally signed by both parties involved in the transaction [119]. Adverse evaluations can be circulated more widely in the trading forum at either trader's choice.

4.5 Addressing the Security and Trust Issues

Provision for secure transactions is a necessary element of an m-commerce trading system. Thus, in order to support security for an ad hoc m-commerce trading system to a sufficient degree for trade to be viable using it, the security and trust service and membership service for the ad hoc m-commerce trading system framework has been designed in the following ways:

Online Identity Establishment - The ad hoc m-commerce trading system frameworks adopts a PGP web of trust scheme as discussed in section 3.7.2. Each trader creates their own trading pseudonym and also public and private key pairs. The traders then establish their own online identity by using their trading pseudonym and photograph as their identity credentials in a self-signed PGP certificate. Each trader's PGP certificate needs to be attested by other parties to ensure the validity of such certificate, as well as to avoid an ill-intentioned trading party from masquerading as others. To minimize the risk that any one certificate signatory is unrecognized or untrusted as an attestor, multiple signatories will usually be required. Traders will verify other traders' certificates based on their knowledge and recommendations from their trusted peers. To make the retrieval of the certificate information easier for verification purposes, traders need to keep their own certificate and other traders' certificates that they have attested or acquired in their local certificate repository. More details about the design of an ad hoc m-commerce trading system's identity support scheme are provided in Chapter 5.

Trust Establishment - To mitigate security issues related to misbehaviour of a trader, the ad hoc m-commerce trading system framework adopts a fully distributed reputation system that employs a sanction-backed mechanism as a means to foster trust among traders. Traders are expected to evaluate their trading counterpart's behaviour in participating in a trade by generating a deal evaluation after the completion or abandonment of each trade. They then digitally sign the deal evaluation and send it to their trading counterpart. Traders can choose to circulate adverse evaluations about their trading counterpart more widely in the trading forum. Traders that have a series of adverse evaluations are open to be sanctioned by other members of the trading forum. Chapter 6 will discuss more details about the design of an ad hoc m-commerce trading system's reputation system.

Attestation Mechanism - Attestation is used as a means for traders to vouch for other parties credentials such as their digital certificates, membership status and reputation reports. It can be an effective way for traders to share their expressions of trust about a particular party in the trading community. It helps to mitigate risks in transactions, especially in situations that involve dealing with unfamiliar traders. As traders are peers who consider each other as equals, the attestation process is done in a P2P manner among traders without involving any higher certification authority and is based on each attestor's knowledge. Any trader can be an attestor to vouch for another trader's credentials. Anyone who trusts the attestor as an attestor, will consider any credentials signed by the attestor to be valid to the extent of that trust.

Group Membership Management - The ad hoc m-commerce trading system framework employs group membership [118] as a means for establishing greater trust and more secure interactions among trading parties in a particular trading forum. It is intended to restrict participation in a trading forum to only those parties that are regarded as reasonably trustworthy by their peers. In order for traders to be a member of a particular trading forum, they have to obtain a membership voucher that has a sufficient number of votes and is digitally signed by recognized group members. The membership voucher serves as a credential that can be used by traders to prove their membership to other members of the forum and it is only valid for a certain period of time. To remain as a member of a particular trading forum, each trader needs to renew their membership voucher periodically when the existing one expires. Any members that misbehave are open to be excluded from the trading forum. Again, any exclusion requires a quorate decision from other members of the trading forum. Details about the design of an ad hoc m-commerce trading system's group membership are discussed in chapter 7.

Sanction-backed Mechanism - The ad hoc m-commerce trading system's reputation system incorporates a sanction-backed mechanism as a strong incentive for traders to behave appropriately especially in fulfilling their transaction agreement and providing truthful deal evaluations and testimonials. Traders that misbehave or have a poor reputation risk being excluded from a trading forum's membership if other traders receive complaints about their misbehaviour. The decision for the exclusion is based on collaborative decision making by a sufficiently large number of forum members, depending on each trading forum's participation and exclusion policy [118].

Security Warning Scheme - A security warning scheme is used as a means to improve the security of an ad hoc m-commerce trading system. It provides a structured process for traders to report, disseminate and act about suspicious behaviour or suspected malpractice in the trading system. Any trader detecting significant breaches of the norms of acceptable trading behaviour by another trader is expected

to notify such misbehaviour to other traders in the trading system by multicasting an alert message, so that they could take the necessary actions and be careful when dealing with the same party in the future. The recipients of such an alert message are then expected to forward it to other traders at later junctions until the message's liveness expires to ensure that a wide scope of traders in that trading community receive such an alert message. This will help the traders in an ad hoc m-commerce trading system to avoid or reduce their risk in transactions. In addition to that, alerts can be used as reminders to encourage traders to behave properly and comply with the trading system's rules and regulations. Traders would be expected to consider the prudence, ethics and legal implications when framing and circulating such alerts.

4.6 Key Characteristics

The ad hoc m-commerce trading system framework is designed to exhibit the following characteristics:

Self-Organization - The ad hoc m-commerce trading system framework is self-organizing, as it can be initiated anywhere by any trader that carries a mobile device with Wi-Fi capability and runs an appropriate m-commerce application. In order for traders to join a particular trading system, they need to set up their mobile device appropriately, i.e. configure the network setting, install and activate an appropriate m-commerce application and generate their online credentials. The self-organization characteristic is important for the ad hoc m-commerce trading system framework as its participants are usually peers with similar roles and device capabilities and thus, it is unlikely that such a trading system could support the existence of a trusted third party administration to manage and control its services. In addition to that, this kind of characteristic is required to provide reliable trading activities due to dynamic participation by the traders in the trading system and unreliable means of communication among them.

Infrastructure-less - In an ad hoc m-commerce trading system framework, as an ad hoc wireless network is used as a communication medium among its participating parties, all of its activities and services such as its membership, security and trust services are handled and managed by its participants using their local and neighbours' resources without relying on any trusted third party supported infrastructure. Traders will keep all their identification, membership and transaction related information in their local repository and exchange it with their trusted neighbours when the need arises.

Low Cost - The ad hoc m-commerce trading system framework is designed to exploit the characteristic of ad hoc wireless networks of being low cost for traders to deploy, maintain and run a trading forum, as well as to participate in the trading activities. Traders only need to purchase a Wi-Fi capable mobile device and install an appropriate m-commerce application which is most likely to be at no or very minimal cost in order to participate in m-commerce transactions, without having to pay any subscription fee to a network service provider. In addition to that, traders can disseminate advertisements for free.

Fully Distributed - The operation of the ad hoc m-commerce trading system framework is designed to be distributed among its participants who are peers that have similar constraints on their devices. Fully distributed characteristics are necessary for an ad hoc m-commerce trading system framework as it cannot be expected that any peer in an ad hoc m-commerce trading forum will always be available and have a high capability mobile device that can act as a trusted server to store relevant information on all other traders in the trading forum. In addition to that, it is unlikely that any peer would be trusted by all other peers in the trading forum to be the anchor point to store such information. Nor is a trusted distributed service supported across all or most of the trading forum members' mobile devices a solution for storing relevant information. Too few nodes in such storage are likely to be present in any local online interaction to guarantee access to relevant data wanted by participants. Thus, it is more practical for traders to store their own trading related information such as their identification details, membership information, trading history and so on in their local repository to ensure that they have the required information when it is needed or requested by other traders.

Dynamic - All services in the ad hoc m-commerce trading system framework need to be designed to be able to handle dynamic and irregular participation by its participating parties, as well as frequent network disconnections among them. As traders can easily join and leave the trading forum, it is important for the ad hoc m-commerce trading system framework to have this kind of characteristic to enable its group membership management service to handle such dynamic membership changes without having to reconstitute the trading group. Any decisions to accept a new member or exclude an existing member from a trading forum are delegated to subsets of the group members and do not require participation by all group members. Furthermore, as the presence of a centralized authority to vouch for the validity of a trader's digital certificate, membership status and reputation reports cannot be guaranteed all the time due to dynamic participation by trading parties, the function of an attestor is also delegated to any members of a trading forum. To lessen the risk that any one certificate signatory is unknown or untrusted as an attestor, multiple signatories will usually be required.

Absence of Authority - As activities in the ad hoc m-commerce trading system framework cannot be expected to involve any authority higher than a peer, the responsibility for managing the services in the ad hoc m-commerce trading system framework especially its membership management service and security and trust service are devolved among members without recourse to trusted parties with delegated authority as no party's presence can be guaranteed in any live trading context. For instance, in the attestation process, any traders who are considered as a trusted peer by other traders can be an attestor to vouch for other traders' certificates, membership, trading history and etc.

Robustness - Due to intermittent participation by members, unreliable means of communication and the absence of dependable enduring infrastructure services, all services in the ad hoc m-commerce trading system framework need to be designed to have failure tolerance support.

Organisational Simplicity - As traders use unreliable communication means to communicate with each other and may make a spontaneous decision to participate in m-commerce transactions when they are on the move, it is important for an ad hoc m-commerce trading system framework to support m-commerce trading protocols that do not require traders to be involved in complicated and time consuming activities to complete protocol stages.

4.7 Ad Hoc M-commerce Trading System Design Comparison

This section compares the ad hoc m-commerce trading system framework with other existing infrastructure-supported m-commerce trading architectures, client/server and P2P m-commerce architectures, and examines several fundamental differences between their properties and implementation.

4.7.1 Ad Hoc M-commerce Trading System Framework vs Infrastructure-Supported Client/Server M-commerce Architectures

Although m-commerce has been recognized as a new way of conducting today's businesses and has grown rapidly in a significant way, most of the existing infrastructure-supported m-commerce systems were designed based on a client/server architecture [181],[182],[34],[101]. Several popular examples of m-commerce systems in-

clude Zillow.com that provides real estate services, Nordstrom.com that provides online shopping services and Target.com that also provides online shopping services [64],[2],[3],[4]. Infrastructure-supported client/server m-commerce systems support complex chains of operations normally by utilizing the Internet [144],[180]. Although infrastructure-supported client/server m-commerce systems share some characteristics with ad hoc m-commerce systems such as location and motion independence, personalization, convenience and etc, their implementation has several fundamental differences from ad hoc m-commerce systems in terms of the following:

Cost for Both Merchants and Customers - A major issue faced by merchants in infrastructure-supported client/server m-commerce systems is that to implement and operate an m-commerce system requires a substantial investment [144],[42],[181],[142], which could be costly for small and medium-size businesses. The costs relate to the the following:

- Cost of designing, developing and maintaining the m-commerce systems; both the front-end and back-end systems.
- Cost of purchasing the necessary software licenses and devices, such as web servers, database servers and so on, in order to implement an end-to-end m-commerce system.
- High initial cost of establishing mobile communication infrastructures using technologies such as GSM, UMTS, GPRS, EDGE etc to better manage the supply chain operations and so on [154].

For customers, they need to pay the mobile network operator or network service provider for the mobile connection service that they use to perform the m-commerce transactions. The charges that they have to pay are normally based on the following factors [160],[159],[153]:

- Airtime - Customers may need to pay connection charges if a long connection is required in order to maintain connectivity to the necessary servers while a transaction completes.
- Number of transactions - Customers often pay based on the number of transactions that they have performed.
- Session - Customers may need to pay for a whole session, regardless of the number of transactions that they have performed.
- Number of messages -Customers pay based on the number of messages that they have sent.

- Combination of all the above - Customers pay a basic rate for the connection and also for the transactions or sessions or messages that they have initiated.

In contrast, an ad hoc m-commerce system only requires traders; both buyers (or customers) and sellers (or providers) to spend lesser amounts in order to implement and operate it. This is due to the fact that traders use an ad hoc wireless network, which is a free wireless communication medium to communicate with each other and they only need to spend the amount of money needed to purchase a mobile device and also appropriate ad hoc m-commerce applications, which might even be obtained for free if they are developed on the popular open source model. They do not need to recompense a third party service provider in order to use the service.

Communication Technology - There are a variety of wireless communication standards that can be used to provide fundamental mobile communication infrastructures to support the activities of infrastructure-supported m-commerce systems, ranging from global, regional to short distance communications, which include Satellite, 4th. Generation (4G) and 3rd. generation (3G) networks, Wireless LAN (802.11 a/b) and Bluetooth [142],[42],[18],[111].

On the other hand, ad hoc m-commerce systems can only be conducted in a small geographical area over ad hoc wireless networks. Currently, the ad hoc wireless communication choices seem to be Bluetooth, ad hoc Wi-Fi and Wi-Fi direct, where only the latter two have sufficient range to be of practical use.

Security Services - Infrastructure-supported client/server m-commerce systems usually rely on the mobile network operator to provide security services to its participating parties to ensure dependable communications and transactions among them.

In contrast, participating parties of ad hoc m-commerce systems need to cooperate with each other using their available resources to support the security services of such trading systems without relying on any infrastructure support from a mobile network operator.

Participating parties - An infrastructure-supported client/server m-commerce system's value chain normally involves entities like customers, merchants or content providers, mobile network operators, financial institutions and possibly other entities [144],[42],[69],[167],[160]. Among the entities, a mobile network operator's role is vital in the whole infrastructure-supported m-commerce value chain. Its role is not only to just provide mobile communication infrastructures for the other entities to communicate but can be more dynamic and complex such as to offer a mobile portal or to act as an intermediary or a trusted third party for security services [160].

However, in an ad hoc m-commerce framework, its transactions only involve two main entities; customers (or buyers) and suppliers (or sellers). These two entities are peers with a similar role that communicate and cooperate with each other to carry out the m-commerce transactions and also handle its security services, without any infrastructure support from a mobile network operator.

Applications' Aim - Most of the existing infrastructure-supported client/server m-commerce applications seem to be aimed at more formal and profit-based trading, especially in the business-to-consumer (B2C) and business-to-business (B2B) market [154],[68],[156],[144]. These kinds of trading sometimes require the m-commerce systems to be linked to financial institutions in order to support mobile payment.

Whereas, ad hoc m-commerce applications suit more informal or casual trading among a group of local people that are in close proximity with each other and involve the trade of digital resources or items that do not have large monetary values. Local trading means that it is practical for traders to have a physical meeting with each other to inspect and swap goods and to make payment for items that are being traded between them. To link ad hoc m-commerce systems to financial institutions or the Bitcoin block chain to support mobile payment among traders might be challenging due to the infrastructure-less nature of an ad hoc wireless network or the inability to guarantee the presence of trusted third parties to underpin online payment processes.

Target Users - Infrastructure-supported client/server m-commerce systems target a wide range of users which include businesses and end-users that might be located globally or locally. In contrast, ad hoc m-commerce systems target only end users that are located in the same area and within the coverage of Wi-Fi or Bluetooth.

The fundamental differences between the implementation of ad hoc m-commerce systems and infrastructure-supported client/server m-commerce systems as discussed above are summarized in Table 4.1.

	Infrastructure-Supported Client/Server M-Commerce	**Ad Hoc M-Commerce**
Cost		
Business Initial Cost (Merchants or Content Providers or Sellers)	Large Investment	Free or Small Investment
Access Charge (Customers or Buyers)	Mobile Service Charges / Free Wi-Fi Zones	Free
Communication Technology		
Wireless Communication Standards	GSM, TDMA, CDMA, EDGE, GPRS and etc.	Ad Hoc Wi-Fi, Wi-Fi Direct, Bluetooth
Service Coverage	Long Range	Short Range
Security Services		
Mobile Network Operator Support	Yes	No
Participating Parties		
Main Entities	Customers, Merchants Mobile Network Operators, Financial Institutions etc.	Traders (Buyers, Sellers, Swappers)
Mobile Network Operator Involvement	Essential	None
Applications' Aim		
Type of Trading	Formal and Profit-based (B2C or B2B)	Informal or Casual (Person-to-Person)
Online Payment Support	Possible	Possible in Future
Target Users		
Type of Users	Businesses and End Users	End Users and Local Market Traders
Scope	Wide Area Globally or Regionally	Small Area within Wi-Fi or Bluetooth Coverage

Table 4.1: Fundamental differences between ad hoc m-commerce and infrastructure-supported client/server m-commerce

4.7.2 Ad Hoc M-commerce Trading System Framework vs Infrastructure-Supported P2P M-commerce Architectures

P2P technology such as JXTA from Sun [155] and .Net from Microsoft [10], has enabled infrastructure-supported m-commerce systems to be implemented based on P2P architectures. Some examples of infrastructure-supported m-commerce systems that were designed based on P2P architectures can be seen in the current implementation of digital content exchange or media distribution applications [36],[17], such as Mobile eDonkey [17],[74] and IMS Mobile P2P [93],[98]. A number of recent P2P schemes have been proposed and developed to carry out Internet-based e-commerce applications in cellular mobile environments [17],[115],[137],[177],[21]. Most of the proposed schemes are based on a hybrid P2P architecture, where the network still utilizes central entities and it consists of two types of nodes; super nodes and ordinary nodes. The super nodes hold most of the network overhead and the ordinary nodes need to be connected to one of the super nodes in order to communicate with the other peers.

Although the design of both infrastructure-supported P2P m-commerce and ad hoc m-commerce is based on a P2P architecture that allows their participating parties to manage and control the operation of such trading systems, there are several fundamental differences between them in terms of the following:

Cost - The cost for the users to participate in infrastructure-supported P2P m-commerce may not be as high as with client/server m-commerce, but the users still need to pay some network access subscription fees to a mobile network operator, which is not required with ad hoc m-commerce.

Communication Technology - Similar to infrastructure-supported client/server m-commerce, there are several wireless communication standards provided by mobile network operators that can be used by the users to participate in infrastructure-supported P2P m-commerce such as GSM, GPRS, EDGE and High Speed Packet Access (HSPA). Thus, users may experience the same network incompatability and adaptation problems as in client/server m-commerce. However, users of ad hoc m-commerce do not face similar diversity of choice in supporting communication protocols.

Architecture - As mentioned above, most of the P2P schemes that have been proposed or developed for infrastructure-supported P2P m-commerce were designed based on a hybrid P2P architecture that utilizes centralized entities and place most of the network overhead on the super peers. In this case, the super peers need to have higher device capabilities than the ordinary peers in order to support the

operation of such trading systems. In contrast, the ad hoc m-commerce framework is designed based on a pure P2P architecture where all peers are similar in terms of their role and device capabilities.

Security Services - Although infrastructure-supported P2P m-commerce allows its participating parties to control its security services such as in distributed reputation systems and so on, communications among them still require network infrastructure support from a mobile network operator. On the other hand, as mentioned in Section 4.7.1 above, participating parties in an ad hoc m-commerce system communicate and cooperate with each other by utilizing their available resources to control the security services of such trading system without relying on any infrastructure support from a mobile network operator.

Table 4.2 summarizes the fundamental differences between ad hoc m-commerce and infrastructure-supported P2P m-commerce.

	Infrastructure-Supported P2P M-Commerce	**Ad Hoc M-Commerce**
Cost		
Access Charge (Customers or Buyers)	Mobile Service Charges / Free Wi-Fi Zones	Free
Communication Technology		
Wireless Communication Standards	GSM, GPRS, EDGE etc.	Ad Hoc Wi-Fi, Wi-Fi Direct, Bluetooth
Service Coverage	Long Range	Short Range
Mobile Network Operator Involvement	Essential	None
Architecture		
P2P Architecture	Mostly Hybrid P2P	Pure P2P
Security Services		
Mobile Network Operator Support	Yes	No

Table 4.2: Fundamental differences between ad hoc m-commerce and infrastructure-supported P2P m-commerce

4.8 Conclusion

An ad hoc m-commerce trading system framework provides a novel paradigm for pure P2P m-commerce. It includes features and characteristics that are different from infrastructure supported m-commerce, especially the client/server based architecture, as the discussion above has pointed out, although they share some similar properties. The unique characteristics of ad hoc m-commerce framework reflect its advantages and its drawbacks.

The process of designing and developing ad hoc m-commerce services and applications is inherently more complex and challenging, as compared to infrastructure-supported m-commerce (both client/server and hybrid P2P based architectures), due to the fact that they are executed on resource constrained devices and in an environment that is dynamic and cannot rely on any infrastructure support from a network service provider or any authority higher than a peer. Cost remains as an important obstacle in infrastructure-supported m-commerce implementations, either client/server or hybrid P2P based architectures.

From the above comparisons, it is seen that ad hoc m-commerce framework has the potential to provide an alternative way for traders to perform m-commerce trading. However, as ad hoc m-commerce has several unique characteristics that make it different from infrastructure-supported m-commerce, application developers need to weigh considerations carefully when designing and developing its services and applications.

Chapter 5

Online Identification with a Fully Self-Organized PGP Certificates

5.1 Introduction

Support for online identity establishment is a crucial element in a security and trust service for an ad hoc m-commerce trading system. It provides assurance for traders that they are communicating, collaborating, carrying out transactions, managing membership and establishing trust relationships with known other parties. Such support not only protects traders from attacks based on identity disguise but can also be used to protect the authenticity, integrity, confidentiality and non-repudiation of the information being exchanged among traders throughout the network, as well as to allow traders' reputation to be shared within the group and support membership in a trading system. A tight binding between an online identity and its reputation enables traders to assess the behaviour and trustworthiness of each trader as well as to favour trustworthy and reputable parties to trade with while avoiding dubious or untrustworthy ones in order to keep transaction risks low. The binding between an online identity and its membership data helps traders to determine the validity of each member's membership status and also each message sent by them in collaborative decision making processes for group membership management. This enables participation in a particular trading system to be restricted to only those parties that are considered to be reasonably trustworthy by other peers in the trading system.

Public key cryptography, via digital certificates provide a means for traders in an ad hoc m-commerce trading system to establish their online identity. A digital certificate enables traders to verify the identity of each party in a trading system. Used in conjunction with encryption, it provides assurance that the messages being exchanged among traders are authentic. However, the validity of the identity

credentials in a digital certificate will only be accepted by the relying parties if it is signed directly or indirectly by a recognized trusted third party. In addition to that, public key cryptography, if it is not implemented in a proper manner will create vulnerabilities that will undermine the security and functionality of the trading system, as discussed in Section 3.3.5.

This chapter starts by examining forms of online identity in the context of online trading in Section 5.2 and then discusses the online identity establishment in an ad hoc m-commerce trading system in Section 5.3. Significant related work is critically assessed in Section 5.4. Section 5.5 presents the conceptual design of an identity support scheme for a security and trust service for an ad hoc m-commerce trading system. Section 5.6 presents a security analysis of the proposed identity support scheme. Several recommendations on things that a trader should do when dealing with digital certificates are discussed in Section 5.7 and finally, Section 5.8 concludes this chapter.

5.2 Online Identity

In online trading, traders are represented by online identities. An online identity refers to a social identity that is established by users as a means to represent themselves in online communities. The main choice here seems to be between using their real identities such as their legal name, date of birth and home address, or a trading pseudonym to represent themselves online. Real identities are predominantly used in trading for items like houses and cars where legal documentation of ownership is important to have. Other forms of trading like buying goods in shops don't require identity establishment unless electronic payment is needed. Traders may choose to use a trading pseudonym if the trading context that they participate in offers no reason for them to provide their real identity, in terms of legal documents or otherwise.

The use of a trading pseudonym would enable traders to participate in online trading incognito. It would also allow traders to keep their trading behaviour discrete and thus protect their privacy. A trading pseudonym enables traders to create an identity that is separate from their personal life and this will allow them to interact and trade with some degree of confidence without fear that their real identity will be stolen, abused or revealed. Furthermore, it would enable traders to project a persona that was distinctive. For example, a pseudonym of Honest Eddy or the Professor could signify a style of approach to trading that reinforces a reputation they wish to maintain. The real identity of a trader in terms of their legal name, date of birth and home address is not necessarily a relevant issue in online trading

if electronic payment is not an issue. Traders can still build reputations in their trading pseudonyms through their trading histories and interactions with others, without linking their real identity to the pseudonym. The reputation of a trading pseudonym can be compromised just as easily as the reputation associated with a real identity. So the value of maintaining that reputation can act as a strong disincentive to abusing a trading pseudonym. By linking together reputation to a trader's pseudonym, the trustworthiness as well as future behaviour of that trader can be evaluated and predicted as long as a persistent identity is used. Pseudonyms make things harder where parties seek legal redress against criminal trading practices or against torts (contract violations) in civil law. However, in casual local trading such recourses to law are rare and anyway the problem of converting a trading pseudonym to the real identity behind it is not insuperable.

In ad hoc m-commerce trading systems, using real identities would create a problem of verification. Attestors of such identities would have to assure themselves that a trader was entitled to call himself by his purported legal name, was actually born on the stipulated date and genuinely resided at the stated address. Performing such checks adequately is tricky, requires the careful perusal of documentation and requires skills in detecting fraudulent ID papers that ordinary parties like other traders would not normally be expected to have. However, in practice, casual trading attestors want to attest an identity established by a recognised appearance and a recognised form of address for trading purposes. What the subject's legal name is or when they were born or where they really live is beside the point. Also, using real identities can make it harder for traders to maintain secrecy about their engaging in particular transactions. Lack of secrecy can threaten a trader's privacy, put them at risk of harm from hostile competitors or even compromise the profitability of deals that they undertake. In addition to that, some traders may have legal name that is uncommon to a certain community or difficult to spell or pronounce. The use of names that are common in a particular community or easier to spell or pronounce as a trading pseudonym can help traders to develop a presence that others can recognize and remember easily, which could subsequently draw a more positive response from other traders in that community. There is also a possibility that several traders have the same legal name such as same first name and surname, which will make it difficult for other traders in that community to distinguish the right trader they're going to trade with. A trading pseudonym will give the opportunity for those traders to have a name that is different from with each other, which can help others to recognize them as a different person easily.

However, allowing pseudonyms raises the issue of whether it allows traders to create multiple identities or change their presented identity too easily. Traders might also try to hide their relation to a particular action like an attestation or vote and thus

avoid being held accountable for that action. To prevent such issues in ad hoc m-commerce trading systems requires robust identification of traders. Robust means of identification will not only protect traders from attacks aimed at identity disguise, but also lets other elements of a security and trust service function properly and effectively.

5.3 Online Identity Establishment in an Ad Hoc M-Commerce Trading System

Due to the infrastructure-less nature of an ad hoc wireless network, frequent network disconnections and irregular participations by its members, an ad hoc m-commerce trading system cannot rely on a network service provider to act as a CA nor can it rely upon any particular trusted party being present at each trading session to serve as a CA. The ad hoc nature of such trading means it can happen anywhere between any subset of the membership. What seems to be needed is some kind of devolution of the CA function over all the membership. Thus, a web of trust scheme using PGP certificates might be such an alternative way for traders in such trading system to establish their online identity in a fully self-organized manner as it would allow traders to generate their own digital certificates and collaborate with each other to handle the verification process of such certificates without relying on a common omnipresent CA or set of CAs to provide such services.

5.4 Related Work

A number of research studies have been done on public key management in ad hoc wireless networks based on a PGP web of trust scheme [79],[31],[94],[163],[178],[45],[170]. Capkun et al. in [31] have proposed a fully self-organized public key management scheme that allows users to generate their own public key pairs, issue digital certificates to other users and also perform authentication with each other by merging their local certificate repositories. The users then evaluate the authenticity of the public key based on the certificates available in the merged repository. Interesting aspects of this approach are that it enables users to control the security settings of the system and also to perform key authentication based on the available information in each user's local repository. In addition to that, it does not require participation by all users during the authentication process. This approach seems to be suitable for ad hoc m-commerce due to its self-organized and distributed characteristics. However, its certificate renewal mechanism, which requires the same issuer

to issue a new updated version of certificate to the same user, would not be appropriate in ad hoc m-commerce as regular participation by trading parties cannot be guaranteed in such trading community. Traders with expired certificates would be at serious risk of having to wait for a long time in order to get in contact with their original certificate issuer. They might not even ever be able to get in contact with those issuers if those issuers no longer participate in the trading system or have been excluded from the trading group.

Dahshan and Irvine in [45],[46] have proposed a similar approach where users create their own public key pairs and issue digital certificates to their neighboring nodes. Users store their own certificate and also the certificates that they have issued to others in their local repository. The difference is that their approach allows users to perform authentication through at least two independent certificate chains. For example, node A wants to authenticate the public key of node D. Thus, node A has to acquire a chain of valid certificates from its node to node D. The first certificate in the chain must be issued by node A and the last certificate holds the public key of node D, as shown in the certificate chain in Figure 5.1. The in-between certificates will be verified using the public key of the previous certificate in the chain. This approach also seems to be practical to be applied in ad hoc m-commerce due to its self-organized, P2P and distributed characteristics. However, requiring the use of two certificate chains to verify the validity of a certificate seems too demanding for ad hoc m-commerce as the chance of two trading parties not known to each other not having two independent certificate chains between their certificates seems quite likely in such a dynamic and fragmented trading community.

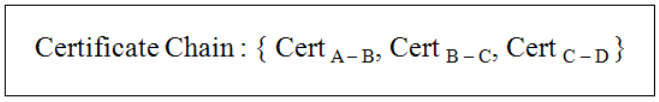


Figure 5.1: A certificate chain

Li et al. in [94] have proposed an approach that utilises a self-signed public key certificate and also the broadcasting property of radio communications to distribute a public key certificate among all nodes in the network. In their approach, it is assumed that every honest node joins the network with a unique network identity (ID) and is equipped with an omni-directional antenna for network communications. A node distributes its public key certificate to other nodes in the network using two processes; neighbourhood certificate distribution and multi-hop certificate distribution. Nodes within two hops of each other exchange their certificates by using a neighbourhood certificate distribution process while nodes that are more than two hops away with each other exchange their certificates using a multi-hop certificate distribution process.

Every node that first joins the network will distribute its self-signed certificate using a neighbourhood certificate distribution process by broadcasting a request message that includes its certificate to its 1-hop neighbours. The receiving nodes validate the request message by verifying the sender's digital signature with its public key in the request message. The receiving nodes then update their neighbourhood certificate and network certificate tables and rebroadcast a reply message that includes their public key certificate and also the public key certificates of all their 1-hop neighbours. The initial sender then updates its neighbourhood certificate and network certificate tables according to the information in the reply message. Other nodes that receive the reply message will not rebroadcast the message, but will instead update their neighbourhood certificate and network certificate tables accordingly if there is a new certificate. After a defined time, the initial sender will send an update message that contains its public key certificate and all its 1-hop neighbours' certificates to all its 1-hop neighbours. This update message is to ensure that all its 2-hops range neighbours receive its public key certificate, in case there are new nodes that have just joined the neighbourhood. The verification of public key certificates is done through neighbourhood monitoring. A node can verify that its certificate is distributed correctly to both its 1-hop and 2-hop neighbours by hearing the message that its 1-hop neighbours rebroadcast. If it is noticed that its certificate was published incorrectly, then it will notify other nodes in the network.

The multi-hop distribution process complies with the rule that each intermediate node will not rebroadcast a message that has already been transmitted by its two 1-hop neighbours. The intermediate nodes verify that the message they received has not been altered by the preceding two nodes, as the two nodes are their 1-hop and 2-hop neighbours and thus, they have their certificate information.

Two interesting aspects of this approach are that it allows the operation of public key management to be fully organized by the nodes themselves without relying on any online trusted third party and it can adapt to the dynamic changes of neighbour relationship and network membership caused by node movement. However, this approach does not discuss any mechanism to vouch for the validity of the self-signed certificates. A self-signed certificate needs to be attested by another party that is trusted to some sufficient degree by its relying parties to verify the validity of its public key and identity information binding, which is important to prevent identity-related issues like identity spoofing and Sybil attacks. In ad hoc m-commerce , it is a necessity to attest the validity of a self-signed certificate as there is a possibility that a trader's pseudonym may not be unique and there is no inherent association between a public key and the identity credentials listed in such a self-signed certificate. Another issue with this approach is that each node has to store the certificates of all the neighbhours within its two hops range as well as the certificates of all avail-

able nodes in the network that it knows. It may not be convenient or even practical for ad hoc m-commerce traders with limited storage capacity device to store such certificate information as they need to store other information as well, such as their trading history, transaction-related information, group membership information and so on.

Although some of the properties in the solutions proposed by the above related work seem suitable to be applied in ad hoc m-commerce, none of them has proposed a certificate attestation mechanism that is suitable overall for the nature and requirements of ad hoc m-commerce. It seems that an ad hoc m-commerce trading system requires a scheme that allows its participating parties to collaborate to establish their online identity using PGP digital certificates and handle the attestation process of those certificates in a fully P2P manner, without any mediation of a CA. The scheme should also support a self-revocation mechanism.

5.5 Design

This section presents the identity support scheme for a security and trust service for an ad hoc m-commerce trading system that employs a public key cryptographic mechanism in a fully self-organised manner, where a trading pseudonym and photograph are used as identity credentials in the PGP certificate. The scheme lets participating parties collaborate in a P2P way to establish their online identity without any mediation of a CA. It is assumed that:

- Traders maintain their own local certificate repository that contains their certificate and other traders' certificates that they have attested or acquired.
- Traders must only use a single trading pseudonym in this trading community at any time unless a pseudonym clash is discovered. To minimise the risk of a pseudonym clash, traders are expected to check for this possibility against all trading pseudonyms that they have heard of, before creating their trading pseudonym.
- Traders' physical appearance will change with time.
- Certificates have a limited validity period of a few years or less (e.g. 4 years). This constrains the period in which identity fraud is possible should a certificate compromise occur. Traders are expected to renew their certificates before the expiration date occurs. Each certificate will have a grace period for its renewal, for example, a grace period of 3 months before or after the expiration date. Thus, a certificate that has expired is allowed to be renewed if it is still within the grace period for renewing the certificate.

- Traders must change their public keys every time they change or renew their certificate.
- Traders may have multiple public keys that are all current but only one key is used at a time to bind their identity credentials in a digital certificate.

5.5.1 The Creation of Public/Private Key Pairs

Using PGP technology [9, 10], each trader in an ad hoc m-commerce trading system will create their own private-public key pairs locally and then store the keys in encrypted form in two separate key rings in their local repositories.

5.5.2 The Generation of Digital Certificates

Traders will also generate their own self-signed digital certificates locally in the form of PGP certificates. Each certificate will contain at least the following information:-

- Type of certificate. Traders are required to choose one of the following three types of certificates when they are generating their PGP certificates:
  - ***"New"*** if they want to generate a completely new certificate.
  - ***"Renew"*** if they want to renew their existing certificate.
  - ***"Update"*** if they want to revoke their existing certificate.

  To renew or update a certificate, traders are required to send together their old certificate when requesting other traders to vouch for the validity of the new certificate.
- The certificate holder's public key.
- The certificate holder's identity credentials which include a trading pseudonym and photograph.
- The digital signature of the certificate owner.
- The certificate's validity period. Each certificate will be issued with a standard limited validity period. Certificates need to be time limited to some degree such as a few years because turnover in the actively participating parties in a trading forum is expected to be high and the signers of certificates are increasingly likely as time passes to cease to be part of the community. Also aging and weight change make mismatches between physical appearance and

photo become increasingly likely and the risks that a user's private key is compromised grow with time. Short validity periods of a year or less for certificates are probably undesirable to avoid the nuisance value and overheads of their renewal too frequently, but 5 years or more seems too long. So 2 to 4 years seems a sensible compromise.

- The digital signature(s) of the certificate's attestor(s) and their certificate identifiers. Multiple recognised signatures on a single certificate give more assurance to the relying parties that the photograph and trading pseudonym in the certificate accurately identify a party with knowledge of the corresponding private key.

5.5.3 The Verification of Digital Certificates

Since there is no inherent association between a public key and the identity credentials listed in the self-signed digital certificates, the validity of such certificates need to be attested by other parties to avoid an-ill intentioned trader from masquerading as others. In ad hoc m-commerce trading systems, participating parties are peers who consider each other as equals. So any peer can vouch for another peer's digital certificate. However, the validity of such a certificate will only be accepted if the relying party recognises a party who has vouched for the certificate as a trustable party. This process is based on the concept of a web-of-trust [9-11]. Anyone who trusts the attestor as an attestor, will consider any certificates signed by the attestor to be valid to the extent of that trust. To lessen the risk that any single certificate signatory is unknown or untrusted as an attestor, multiple signatories will usually be required. Fundamental verification processes in an ad hoc m-commerce trading system include the following two processes; namely attestation and authentication.

5.5.3.1 Attestation Process

The process of verifying the identity credentials and public key binding that reflects an identity in a digital certificate is crucial in order to prevent identity-related threats, especially identity spoofing. Without a reliable attestation process, an ill-intentioned trader could masquerade as another trader by using the identity credentials of that trader. Thus, in an ad hoc m-commerce trading system, traders are required to activate the following automated attestation checks when they receive a request by other traders to vouch for their digital certificates' validity by signing it.

A. Attestation Checks

Below are the steps that should be performed by the trading system's application when the automated checks for a certificate attestation are initiated. A flowchart in Figure 5.2 (page 86) illustrates the step-by-step checks. Traders are expected to take the necessary actions based on the result of each check.

Step 1 - Check whether the presented certificate is a completely new one or a renewal or an update of an earlier one by checking its type.

If the certificate is found to be a completely new one, the trading software will proceed to step 2 to perform further checks on the certificate. Otherwise it will perform the steps that will be discussed in Section 5.5.3.1(B).

Step 2 - Check the self signature of the presented certificate against its public key to ensure that the contents of the certificate were not altered.

If the self signature on the presented certificate checks out, the trading software will proceed to step 3. Otherwise, it will display an alert message that the presented certificate is suspected to have been compromised. Thus, the attestor should refuse to sign it.

Step 3 - Check the trading pseudonym in the certificate against its store of certificates to see if that trading pseudonym has already been used by another party.

If no match is found, the trading software will perform step 4. Otherwise, it will check whether the public key of the presented certificate matches with the public key of the existing certificate.

If there is no match between the two certificates' public key, the trading software will display an alert message that the trading pseudonym has been used by another party. If the alert message shows the photos of two different persons, as illustrated in Figure 5.3 (page 87), then the attestor should refuse to sign the certificate and inform the sender that the presented trading pseudonym is already in use and suggest the use of another trading pseudonym.

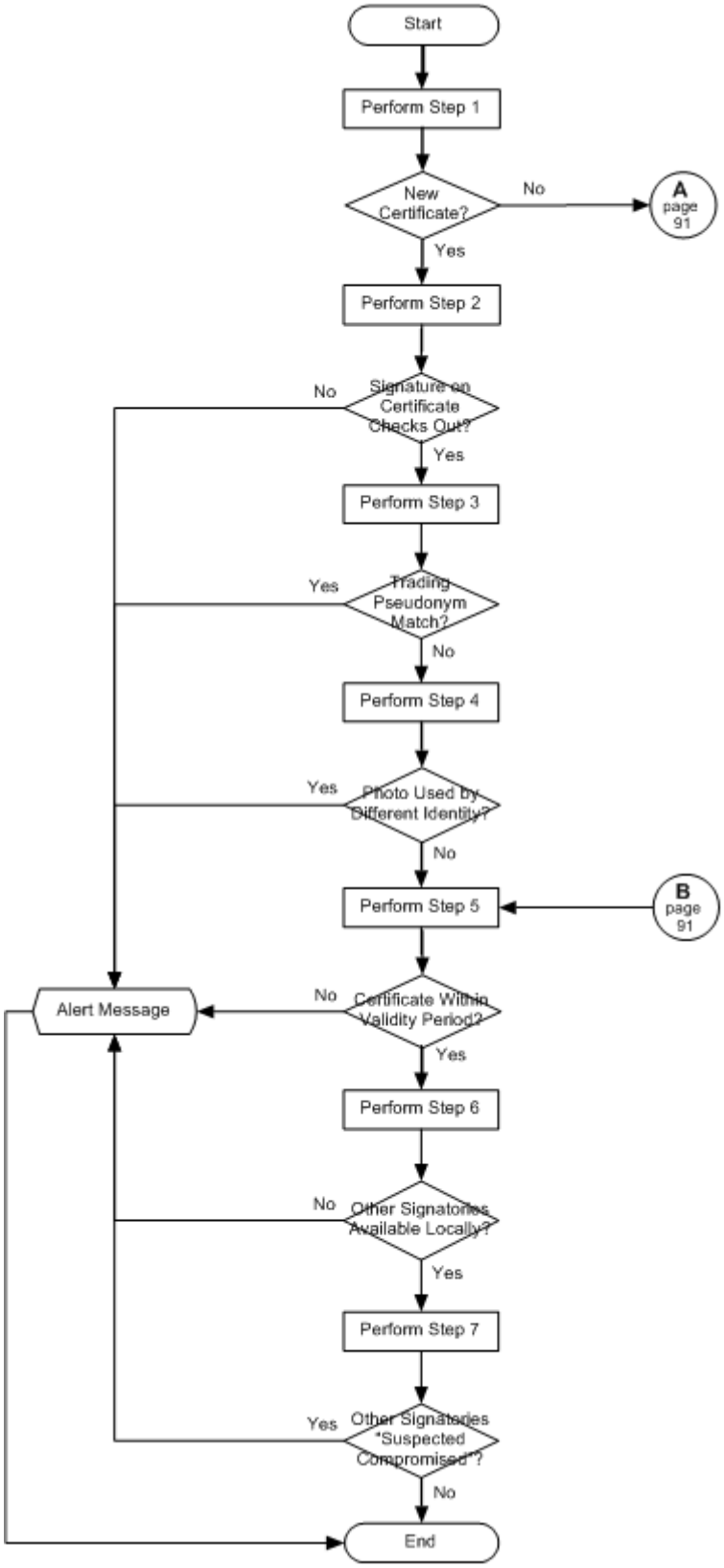


Figure 5.2: A flowchart for the automated attestation checks for a new certificate

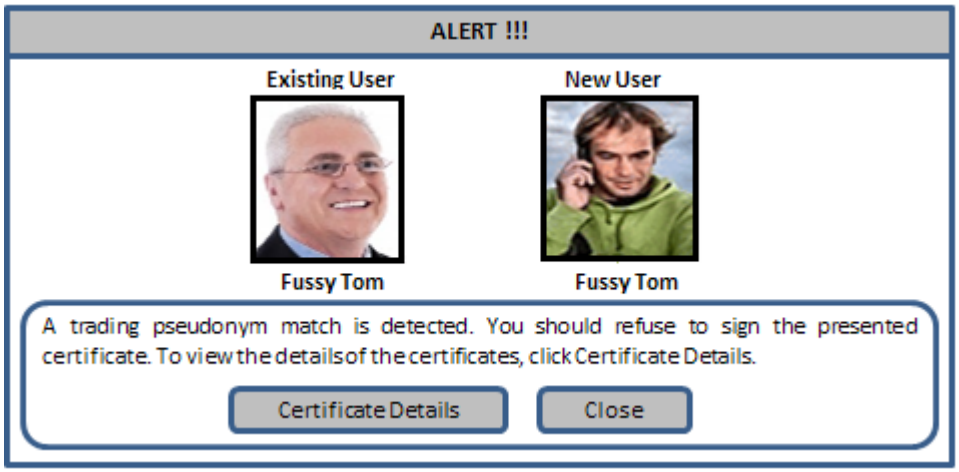


Figure 5.3: An example alert screen for a trading pseudonym match (different photo appearance)

If the photos in the alert message have some or a clear resemblance with each other, as illustrated in Figure 5.4, there is a possibility that both users are the same person. However, in this case, the attestor should also refuse to sign the presented certificate and inform the sender that the trading pseudonym has been used by an existing identity. If the sender claims that he is renewing his old certificate but mistakenly sent it as a new one, then the attestor should inform him to send another request for a certificate renewal where he has to send it together with his old certificate.

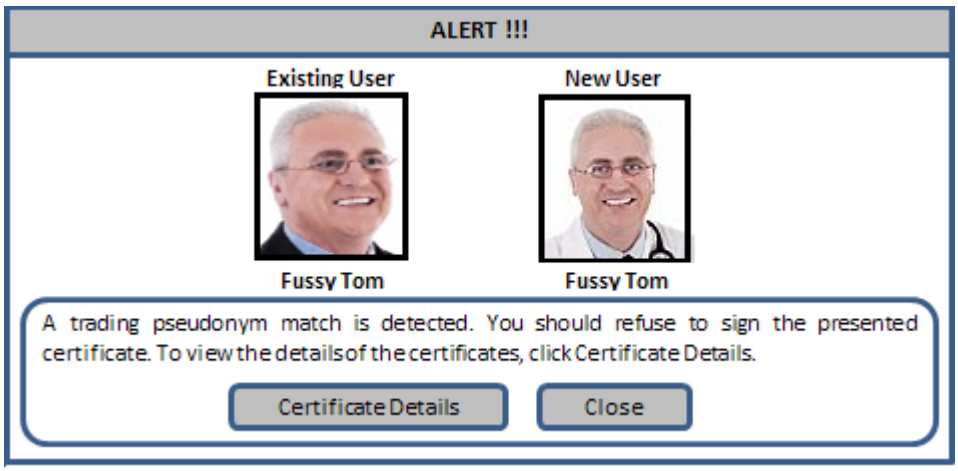


Figure 5.4: An example alert screen for a trading pseudonym match (similar photo appearance)

If the public key of both certificates are found to be matched with each other, the trading software will display an alert message as illustrated in Figure 5.5. In this case, if the photos in the alert screen are sufficiently different from each other, the attestor should refuse to sign the presented certificate as there may have been an attempt by its sender to spoof the identity of an existing party. If the photos have some or a clear resemblance to each other, the attestor should also refuse to sign the

presented certificate. This is because if the sender is renewing his old certificate, he is supposed to go through a proper certificate renewal process.

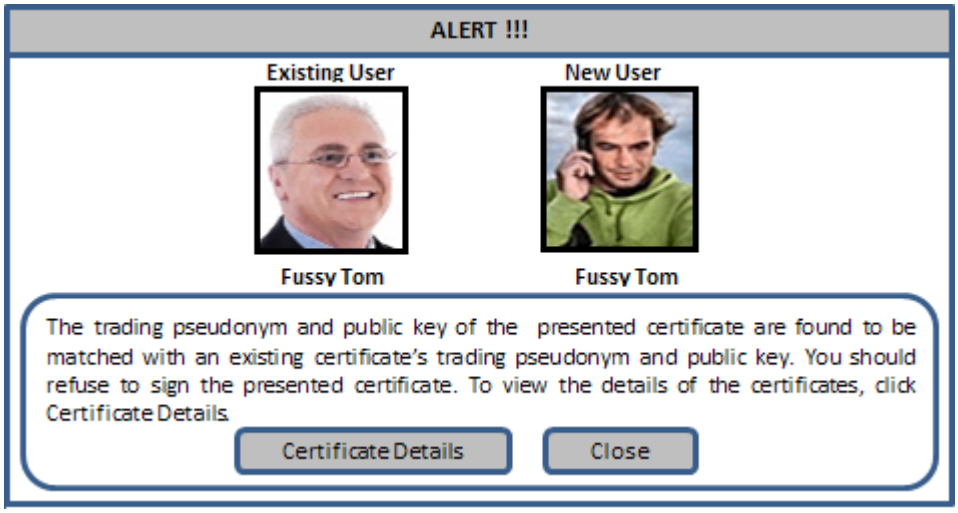


Figure 5.5: An example alert screen for a trading pseudonym and public key match

This step should reduce the likelihood but not prevent the possibility that two or more parties in the same trading system use the same trading pseudonym.

Step 4 - Check the photo in the presented certificate against its store of certificates to see if that appearance is used with a different trading pseudonym.

If no match is found, the trading software will then perform the check in step 5. Otherwise, it will display an alert message as illustrated in Figure 5.6. In this situation, the attestor is expected to perform further checks, which will be discussed in Scenario 1 in Section 5.5.3.1(C). If more than one matches are found, then all the certificates that have similar photograph appearance should also be checked.

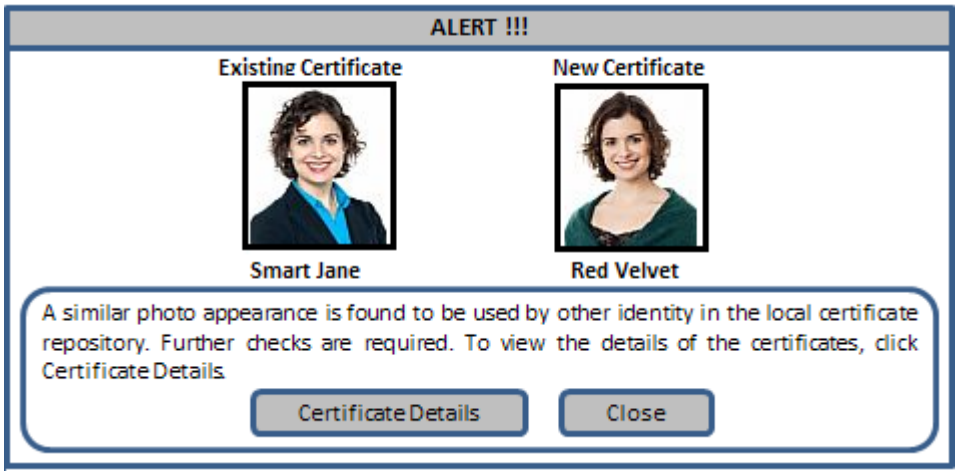


Figure 5.6: An example alert screen for a similar photo appearance used by other identity

Step 5 - Check the validity period of the presented certificate, whether the current date and time is within the validity period.

If the current date and time is within the certificate's validity period, the trading software will then proceed to step 6. Otherwise, it will display an alert message that the current date and time is outside the presented certificate's validity period and thus, the attestor should refuse to sign it.

Step 6 - Check whether the certificate has other signatories whose certificates are available in the local certificate repository.

If the certificate has no other signatories, the trading software will display a message that all checks on the presented certificate are successful, as shown in Figure 5.7. However, the attestor must verify that the owner has the right to use the trading pseudonym by checking with other traders and physically meet the sender to make sure that his physical appearance is similar to the enclosed photo in the presented certificate, before signing the certificate. Otherwise, the trading software will perform step 7.

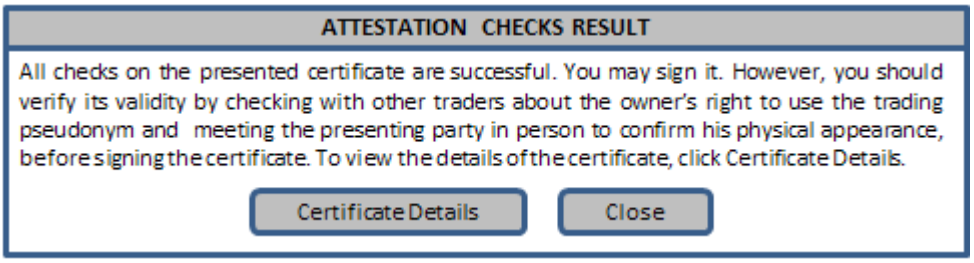


Figure 5.7: An example result screen for a certificate that has no other signatories

Step 7 - Check whether any of the signatories' certificates is recorded as "suspected compromised" in the local certificate repository

If none of those signatories' certificates is recorded as "suspected compromised", the trading software will also display a message as shown in Figure 5.7. In such a case, the attestor may vouch for the validity of the presented certificate by signing it. However, the attestor is expected to perform the same action as discussed in step 6, before signing the certificate.

If one or more of the signatories' certificates are found to be recorded as "suspected compromised", then the trading software will display an alert message as illustrated in Figure 5.8. In such a case, the attestor should be wary about signing the presented certificate.

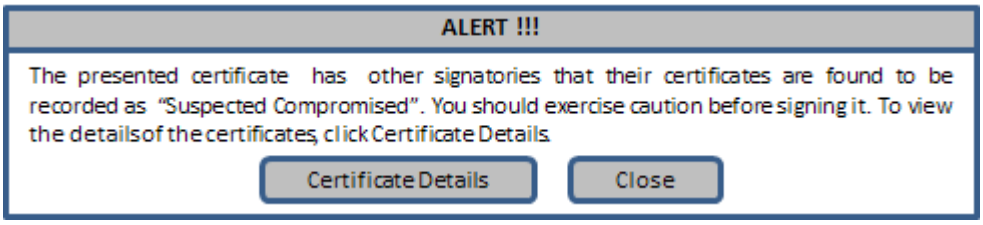


Figure 5.8: An example alert screen for a certificate that one or more of its signatories' certificates is recorded as "suspected compromised"

B. Attestation Checks for a Certificate Renewal or Revocation

The following checks as illustrated in a flowchart in Figure 5.9, will be performed by the trading software when the result of step 1 in Figure 5.2 (page 86) found that the presented certificate is a renewal or an update of an earlier one.

Step 1 - Check whether the self-signature on both the new and older certificates matches with their corresponding public key.

This step is to ensure that the contents of both certificates were not altered. Thus, if the signatures on both certificates check out, the trading software will then perform step 2. If the signature on one or both of the certificates is found to be mismatched with its corresponding public key, the trading software will display an alert message as illustrated in Figure 5.10 (page 92). In such a case, the attestor should reject the certificate renewal or revocation request.

Step 2 - Check the old certificate's trading pseudonym and public key against its store of certificates to see whether there is a copy of that certificate locally.

If there is a copy, the trading software will proceed to step 3. Otherwise, it will display an alert message that a copy of the old certificate is not available locally. Thus, the attestor is expected to verify the validity of the presented certificate by checking with other traders about its owner's right to use the trading pseudonym and meeting the presenting party in person to confirm that his physical appearance is similar to the photo in the presented certificate, before signing it.

Step 3 - Check whether the presented certificate is a renewal or an update of an earlier one by checking its type.

If the certificate type is stated as "renew", the trading software will then proceed to step 4, else it will display an alert message that the presented certificate is found to be an update of an earlier one and further checks are required for a revocation of a certificate. The further checks will be discussed in Scenario 2 in Section 5.5.3.1(C).

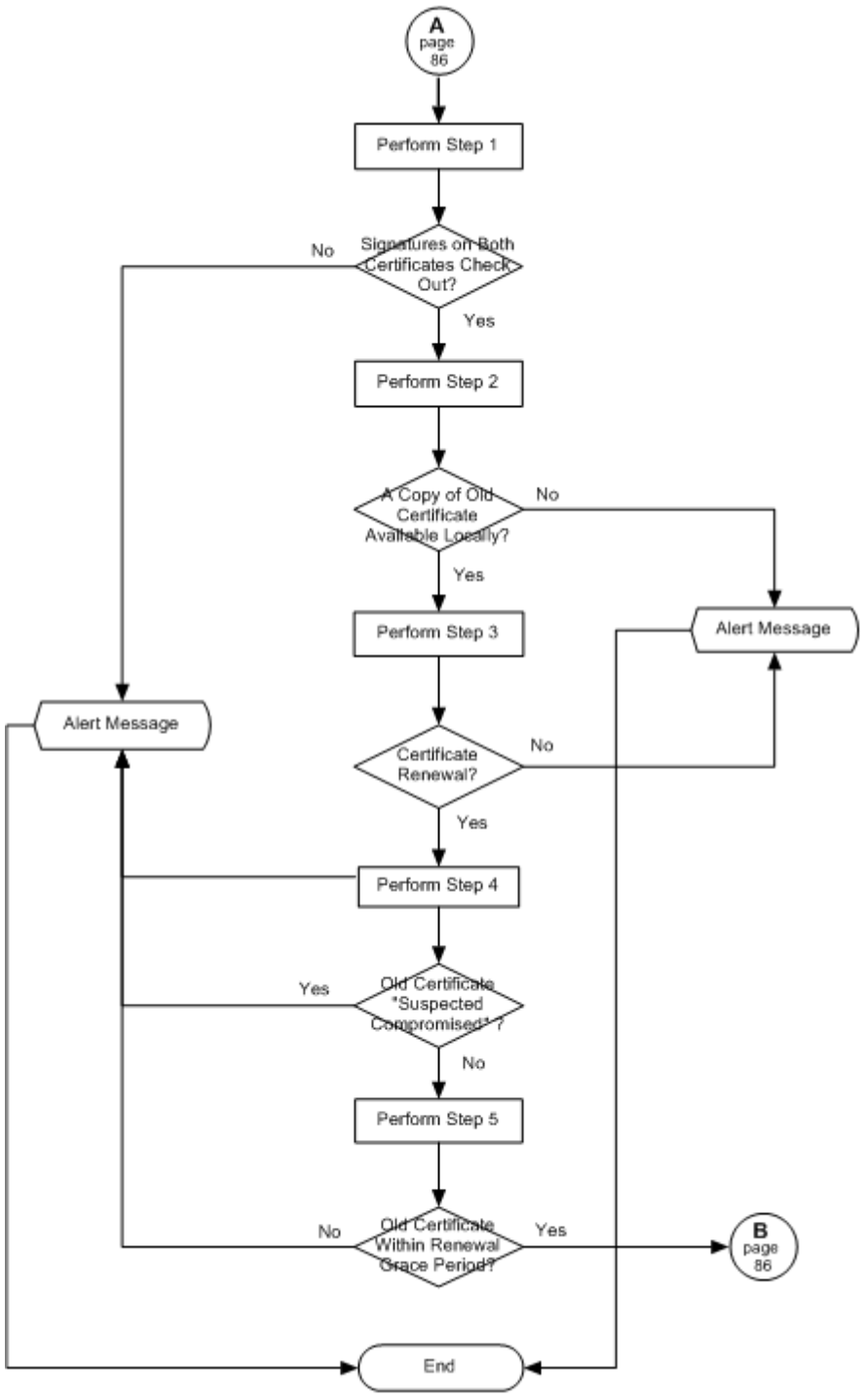


Figure 5.9: A flowchart for the automated attestation checks for a certificate renewal or revocation

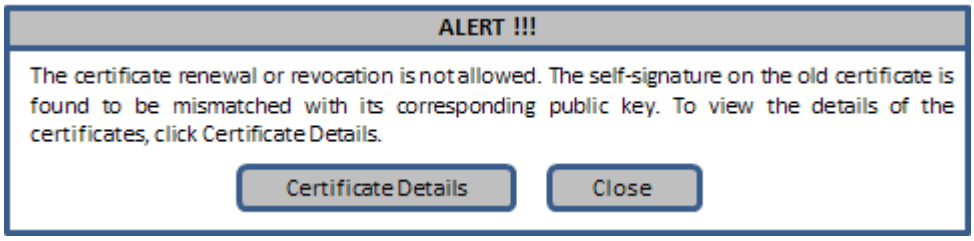


Figure 5.10: An example alert screen for a self-signature on the older certificate is found to be mismatched with its corresponding public key

Step 4 - Check whether the old certificate is recorded as "suspected compromised" in the local certificate repository.

If the old certificate is not recorded as "suspected compromised", the trading software will perform step 5. Otherwise, it will display an alert message that the certificate renewal is not allowed because the old certificate is suspected to have been compromised. The attestor is expected to refuse to sign the presented certificate unless they have good reasons to the contrary.

Step 5 - Check the validity period of the old certificate, whether the current date and time is within its renewal grace period.

If the current date and time is outside its renewal grace period, the trading software will display an alert message that the certificate renewal is not allowed due to the current date and time is outside the old certificate's renewal grace period. Thus, the attestor should reject the renewal request.

Otherwise, the trading software will then perform steps 5 to 7 in Figure 5.2 (page 86). If the checks in these steps are successful, the trading software will then display a result screen that all checks are successful. If the result screen shows that the photos in both certificates have some or a clear resemblance with each other, as illustrated in Figure 5.11, the attestor could verify the validity of the new certificate by signing it.

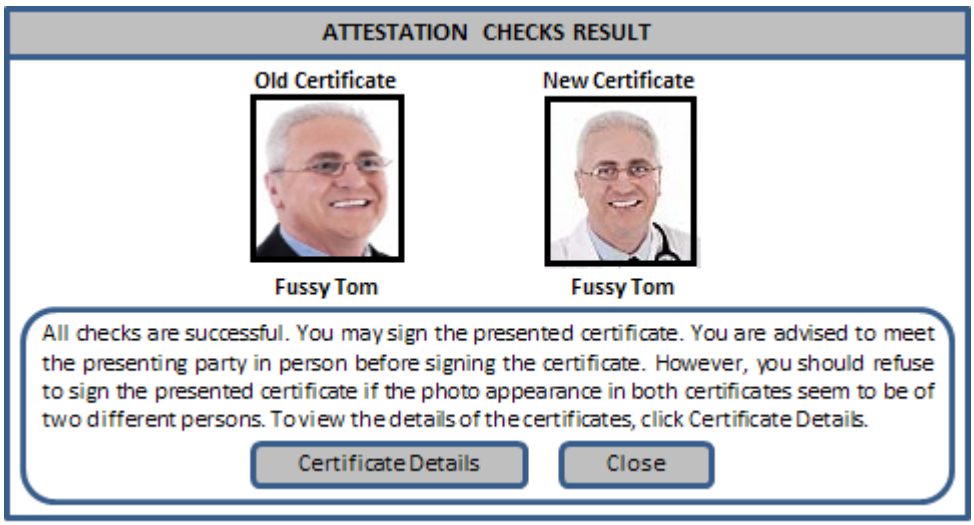


Figure 5.11: An example result screen for successful attestation checks (similar photo appearance)

However, the attestor would normally be expected to meet the sender in person to confirm that his physical appearance is similar to the photo in the presented certificate, before signing it. If the photos in both certificates are found to be sufficiently different from each other, as shown in Figure 5.12, the attestor should refuse to sign the new certificate.

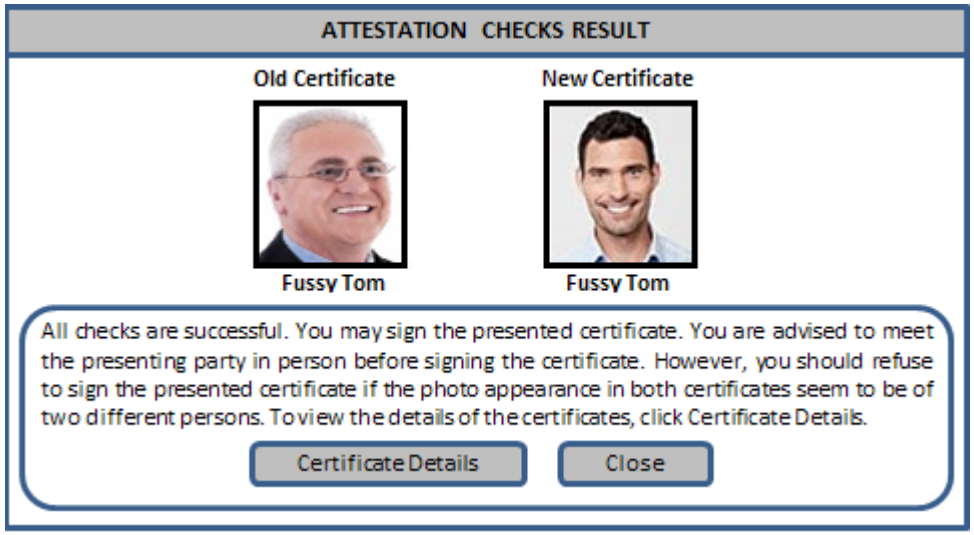


Figure 5.12: An example result screen for successful attestation checks (different photo appearance)

C. Further Checks

As the results of some of the automated checks may not give sufficient information for the traders to decide whether to sign or not a PGP digital certificate that is presented to them, they need to perform further checks to make sure that the certificate that they are verifying prior to attestation is valid and belongs to the person claiming its ownership before signing it. The checks may differ from one situation to another situation, and will be discussed in a series of scenarios below.

Scenario 1 - A situation where the checks done by the trading software in Step 4 in Figure 5.2 (page 86) finds that the photograph in the presented certificate is similar to the photograph in an existing certificate with a different trading pseudonym in the local certificate repository. In this situation, the attestor should perform the following checks:

1) Check whether that existing certificate is recorded as "suspected compromised" in the local certificate repository by clicking at the Certificate Details button in the alert message and then choose to see the detail information and status of the existing certificate.

If the certificate is not recorded as "suspected compromised", the attestor needs to perform step 2. Otherwise, the attestor needs to physically meet the presenting party to see whether his physical appearance is similar to the photo in the presented certificate.

If the physical appearance of that party is sufficiently different from the photo in the presented certificate, then there is a doubt whether they are the same person. Thus, the attestor should refuse to sign the presented certificate as there may have been an attempt by the presenting party to create a fake identity using another party's photograph.

If the physical appearance of the presenting party is similar to the photograph in both the presented and existing certificates, there is a possibility that the presenting party is a genuine trader who wants to create a new identity after his old certificate was compromised. However, in this situation, the attestor should refuse to sign the presented certificate. If the presenting party claims that the existing certificate is also his certificate that was suspected to be compromised, then the attestor should inform that party to go through a proper certificate revocation process in order to have a new certificate. The attestor is also expected to inform the presenting party that he needs to continue to use the same trading pseudonym.

2) Check whether the existing identity is someone they know from personal experience and have interacted with before. If it is someone that they know who has maintained a good reputation, then there may be an attempt by the presenting

party to create a fake identity by using that party's photo. If the existing identity is someone with a suspect or bad reputation before, or someone that the attestor does not have any personal experience with or have never dealt with in any trading or other activities before, then there may be an attempt by the presenting party to have multiple identities. If the existing identity is someone who has been excluded from the trading forum membership, then there may be an attempt to re-enter the trading forum with a new identity. In all cases, the attestor needs to physically meet with the presenting party to check whether his physical appearance is similar to the photo in the presented certificate.

If the physical appearance of that party is sufficiently different from the photograph in the presented certificate, there may be genuine doubt whether they are the same person. In such a case, the attestor is expected to refuse to sign the certificate as there may have been an attempt by the presenting party to create a fake identity using an existing party's photograph.

If the physical appearance of the person bears some or a clear resemblance to the photograph in both the presented and existing certificates, and that party is known to have a bad reputation before or is someone with no reputation yet, or is someone who has been excluded from the trading forum membership, the attestor should refuse to sign the certificate. This is because it could be an attempt by that party to have multiple identities or re-enter the trading forum with a new identity. If that party is someone that is known to have a good reputation before, the attestor should also refuse to sign the presented certificate and inform that party that traders of an ad hoc m-commerce trading system are not allowed to have more than one trading pseudonym.

Scenario 2 - A situation where the trading software checks in Step 3 in Figure 5.9 (page 91) finds that the presented certificate is an update of an earlier one, the attestor is expected to perform at least the following checks before attesting the presented certificate by signing it.

1) Check the reason(s) for the revocation. This can be done by clicking on the Certificate Details button in the alert message. If the reason(s) given is acceptable for a certificate revocation, then the attestor should perform step 2, else the presented certificate should not be signed. Section 5.5.5 will discuss the reasons that are acceptable for a revocation of a certificate.

2) Check whether the current date and time of the presented certificate is within the certificate's validity period. If the current date and time is within the validity period, the attestor should then perform step 3. Otherwise, the presented certificate should not be signed.

3) Compare the photos in the presented and old certificates. This can be done by clicking to view the details of each certificate from the alert message. If the photos in both certificates show some or a clear resemblance with each other, the attestor is expected to meet the presenting party in person to verify that his physical appearance is similar with the photos in both old and presented certificates before signing the presented certificate and marking the old one as "revoked". If the photos in both certificates are sufficiently different from each other, the attestor should refuse to sign the presented certificate.

5.5.3.2 Authentication Process

Certificate authentication is the process of verifying that a particular person presenting a digital certificate is whom he or she claims to be. This process is also critical to prevent identity-related threats. This is because even with a proper attestation process, if the authentication fails, identity spoofing can still occur. Thus, in an ad hoc m-commerce trading system, the following automated authentication checks should be performed by the trading system's application when a trader receives a digital certificate from other trader for trading or other related activities.

A. The Automated Authentication Checks

Below are the checks that should be performed by the trading software during the authentication process of a PGP digital certificate. A flowchart in Figure 5.13 illustrates the step-by-step checks. Traders are expected to take the necessary actions based on the result of each check.

Step 1 - Check of the self signature of the certificate against the certificate's public key.

This step is to ensure that the presenting party has not altered the contents of the presented certificate like the certificate's validity period or its owner's photograph. If the self signature checks out, the trading software will perform step 2. Otherwise, it will display an alert message that the presented certificate is suspected to have been compromised. Thus, the certificate should not be trusted.

Step 2 - Check of the validity period of the certificate, whether the current date and time is within the validity period.

If the current date and time is within the validity period, the trading software will proceed to step 3. Otherwise, it will display an alert message that the current date and time of the presented certificate have been found to be outside its validity period. The recipient is expected not to trust the presented certificate.

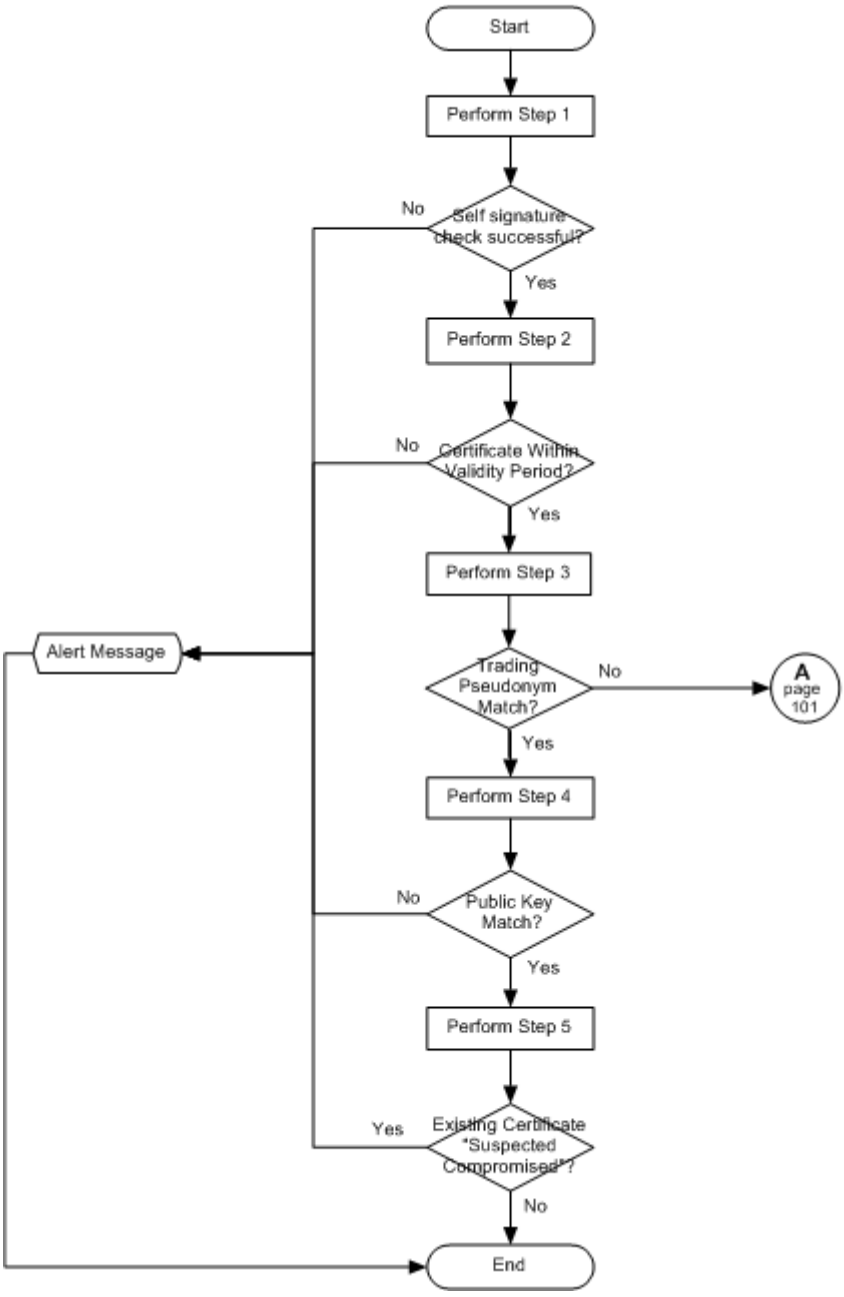


Figure 5.13: A flowchart for the automated authentication checks

Step 3 - Check of the presented certificate's trading pseudonym against its store of certificates to see whether there is an existing certificate with the same trading pseudonym.

If a match is found, the trading software will perform step 4. Otherwise, it will perform further checks on the presented certificate, which will be discussed in Section 5.5.3.2(B).

Step 4 - Check whether the presented certificate's public key matches with the public key of the existing certificate with the same trading pseudonym.

This step is to determine whether the recipient has interacted with the same identity before. If yes, there should be a copy of the presented certificate in the local certificate repository. Thus, if there is a match between the presented certificate's public key with the existing certificate's public key, the trading software will proceed to step 5 to further check the certificate. If not, it will display an alert message as illustrated in Figure 5.14. In such a case, the recipient is expected to compare the photos in both the presented and existing certificates by viewing the details of each certificate.

Figure 5.14: An example alert screen for a certificate that has a similar trading pseudonym with an existing certificate, but different public key

If the photos in both certificates are found to have some or a clear resemblance to each other, the recipient should then meet the presenting party in person to verify his physical appearance. If his physical appearance is sufficiently different from the photos in both certificates, then there may be a genuine doubt whether they are the same person. Thus, the recipient is expected not to trust the presented certificate as there may have been an attempt by the presenting party to spoof the existing party's identity. If the physical appearance of that party is similar to the photos in both certificates, then there is a possibility that they are the same person. Thus, in this case, if the presenting party claims that the presented certificate is a renewed version of the older one and the recipient may have not yet received that certificate renewal notification, the recipient should then ask that party to prove knowledge of the private key corresponding to the older certificate's public key. Failure to do so will cause the recipient to reject the presented certificate.

If the photos in both certificates are found to be sufficiently different from each other, then the recipient should not trust the presented certificate.

Step 5 - Check whether the existing certificate is recorded as "suspected compromised" in the local certificate repository.

If the certificate is found to be recorded as "suspected compromised", the trading software will display an alert message that the presented certificate is suspected to have been compromised and thus, it should no longer be trusted unless the recipient has good reasons to the contrary.

Otherwise, the trading software will display the final result of the checks. The recipient is expected to accept the presented certificate if the photos in both certificates in the result screen show some or a clear resemblance to each other, as illustrated in Figure 5.15.

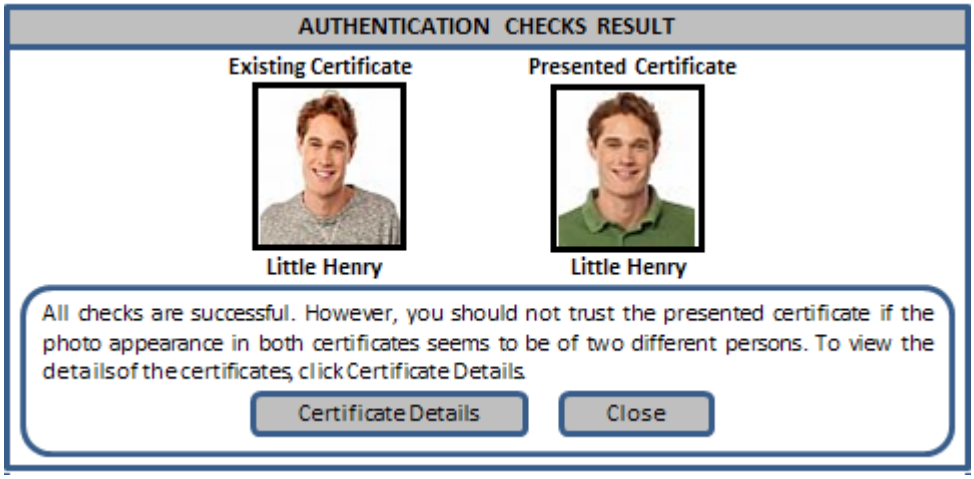


Figure 5.15: An example result screen for successful authentication checks (similar photo appearance)

However, the recipient needs to have a physical meeting with the sender to verify his physical appearance before accepting the certificate. If the photos in both certificates were of two different persons as illustrated in Figure 5.16, then the recipient should not trust the presented certificate.

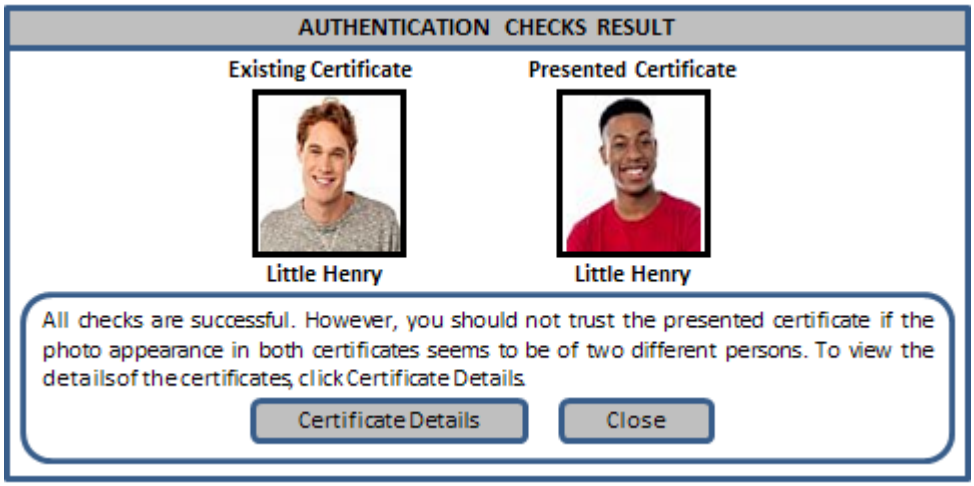


Figure 5.16: An example result screen for successful authentication checks (different photo appearance)

B. Further Authentication Checks on the Presented Certificate

The following checks as illustrated in a flowchart in Figure 5.17, will be performed by the trading software when the result of step 3 in Figure 5.13 (page 97) found that there is no existing certificate in the local certificate repository that has a similar trading pseudonym as in the presented certificate.

Step 1 - Check the photo in the presented certificate against its store of certificates to see if that appearance is used by a different trading pseudonym.

If this check is successful, the trading software will perform step 2. Otherwise, it will display an alert message as illustrated in Figure 5.6 (page 88). In such a case, the recipient is expected to perform further checks on the presented certificate as discussed in Scenario 1 in Section 5.5.3.1 (C).

Step 2 - Check whether the digital certificate of any third parties who have signed the presented certificate are available in the local certificate repository.

If one or more of the signatories' certificates are available locally, the trading software will then perform step 3 to further check those certificates. Otherwise it will display an alert message as illustrated in Figure 5.18. In this case, as the presenting party and the certificate's signatories are parties that the recipient has never interacted with before, the recipient is expected to checks with other traders about the presenting party's right to use the pseudonym and meet him in person to confirm that his physical appearance is similar to the photo in the presented certificate, before relying on that certificate.

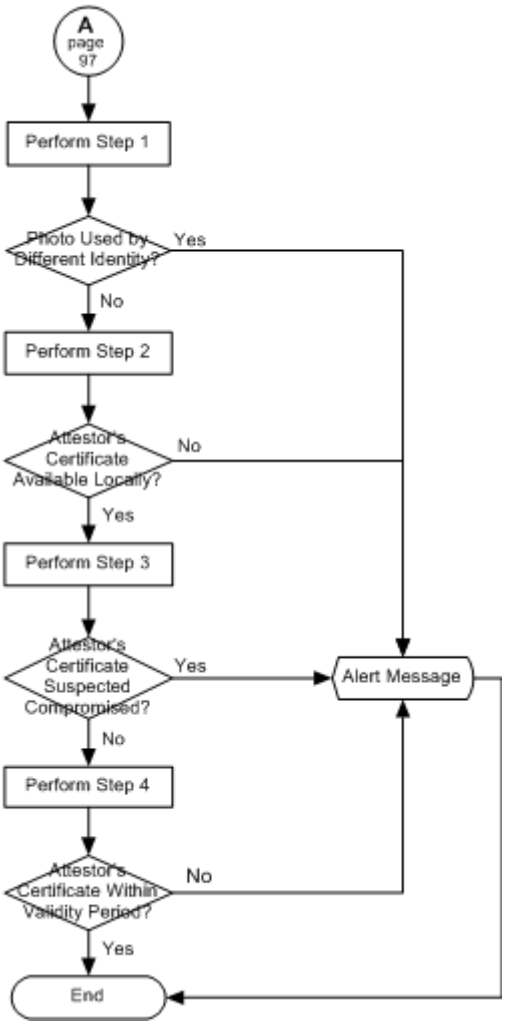


Figure 5.17: A flowchart for further authentication checks on the presented certificate

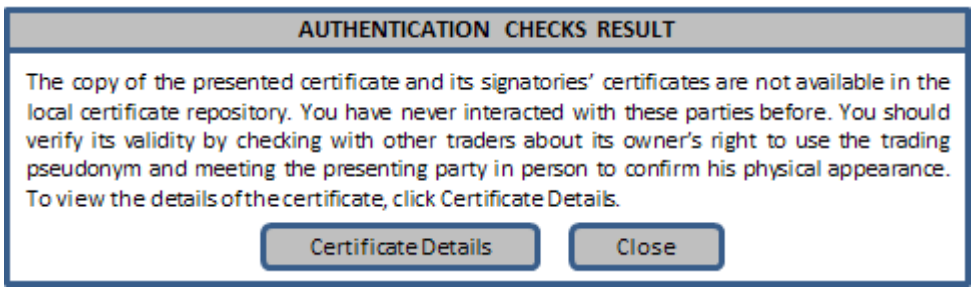


Figure 5.18: An example alert screen when a copy of the presented certificate and its signatories' certificates are not available in the local certificate repository

Step 3 - Check whether any of the signatories' certificates is recorded as "suspected compromised" in the local certificate repository.

If none of the signatories' certificates is found to be recorded as "suspected compromised", the trading software will proceed to step 4. Otherwise, it will display an alert message as illustrated in Figure 5.19. In this case, the recipient should be wary about trusting the presented certificate. The recipient is also expected to check around whether the party in question is known by his pseudonym and physically meet with the sender before relying on that certificate.

Figure 5.19: An example alert screen for a certificate that one or more of its signatories' certificates is recorded as "suspected compromised"

Step 4 - Check whether the signatories' certificates are still within their validity period during which the presented certificate is attested.

If one or more of the signatories' certificates is found to have been expired during the time the presented certificate is attested, the trading software will display an alert message as in Figure 5.20. Thus, the recipient should exercise caution before relying on the presented certificate.

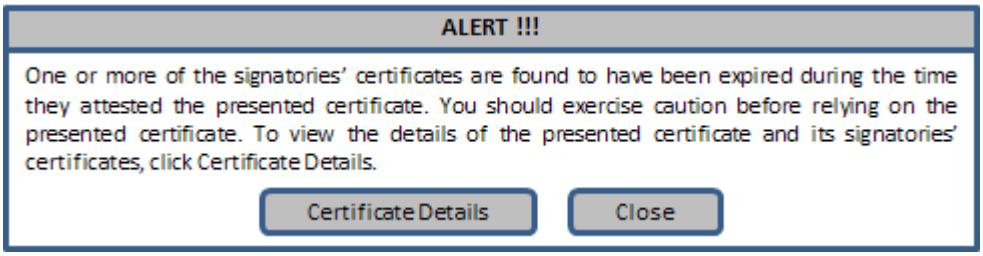


Figure 5.20: An example alert screen for a certificate that one or more of its signatories' certificates is already expired during the time it is attested

Otherwise the trading software will display the final result of the checks as illustrated in Figure 5.21. The recipient may trust the presented certificate if its signatories are considered as trusted key signers. However, as they have never interacted with each other before, the recipient should check with other traders about the owner's right to use the pseudonym and meet him in person to confirm that his physical appearance is similar to the photo in the presented certificate, before relying on that certificate to establish anything with regard to its owner's identity.

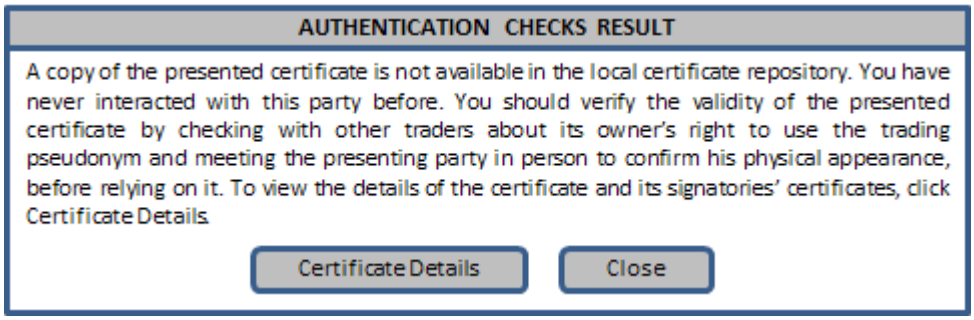


Figure 5.21: An example result screen for a certificate that its copy is not available in the local certificate repository

5.5.4 Certificate Renewal

Certificates are normally created with a restricted lifetime: a start date/time and an expiration date/time. Although an expired certificate doesn't disprove the identity of its presenter, it does raise doubts about the usefulness of the photo and about whether the presenter has had difficulties finding trustable third parties to sign a current certificate for that party. Thus, it is necessary for traders to renew their certificates before the existing one expires or the renewal grace period for the certificate is over. To renew a certificate, a trader needs to perform the following steps:

1) First, generate a new self-signed certificate that binds their identity credentials with a new public key.

2) Second, send a certificate renewal request message together with the newly generated certificate and their older certificate to any traders that they believe to be trustworthy for certificate attestation.

3) Third, multicast a certificate renewal message that is signed by the new and old private keys together with the newly generated certificate and the older certificate to other traders in the trading system.

The receiving parties are then expected to update their local certificate repository with the new certificate, if the checks done by the trading software show the following results. They are also expected to forward the renewal message and its contents to other traders at later occasions until the message's liveness expires to ensure that traders of the trading system are updated with that certificate renewal.

1) Signatures on the renewal message check out. If this check fails, the receiving parties should not trust the new certificate.

2) The trading pseudonym is the same. If not, the new certificate should not be trusted.

3) The photos in both old and new certificates seem to be of the same person. If the photos are sufficiently different, the receiving parties should not trust the new certificate.

5.5.5 Certificate Revocation

Certificates are only useful while they are valid. It is unsafe to simply assume that a certificate is valid forever as it might be compromised before its expiration date arrives. A certificate that has been compromised needs to be revoked. Other reasons why digital certificates may need to be revoked include the following:

- Attestor's certificate is compromised.
- Identity credentials need to be updated. For example, to change an old photograph with a new photograph as the user may have put on a lot of weight.
- A trader has generated another key pair and prefers to use that key instead. It might be longer and promise more security.
- A trader no longer wishes to be a member of a trading system and opt out to exit the trading system forever in a clean way.

5.6 Security Analysis

This section analyzes the means by which the ill-intentioned parties in an ad hoc m-commerce trading system can pose identity-related threats to subvert its security by compromising the proposed identity support scheme. It also discusses on how the verification steps in both attestation and authentication processes help traders to detect and mitigate such threats.

5.6.1 Addressing Identity Spoofing

There are several ways that ill-intentioned parties can spoof other parties identities using PGP certificates, which include the following:

5.6.1.1 Compromising The Attestation Process

With respect to the attestation process, there is always the risk that an ill-intentioned trader misrepresents their identity credentials and tries to masquerade as someone

else. An ill-intentioned trader might, for example;

1) Generate a new key pair and put the public key in a digital certificate using a reputable party's trading pseudonym and photograph, and then self-sign the digital certificate with the corresponding private key. In this scenario, if the certificate is sent as a new certificate and the attestor has a copy of that reputable party' certificate in his local certificate repository, the check in step 3 in Figure 5.2 (page 86) should be able to detect that the trading pseudonym in the presented certificate has been used by an existing certificate with a different public key in the local certificate repository. Thus, the trading software will alert the attestor that the certificate should not be signed because its trading pseudonym has been used by another party, as illustrated in Figure 5.4 (page 87). However, as the photo appearance in the presented certificate has some resemblance to the photo in the existing certificate, the presenting party might claim that he is renewing his older certificate but mistakenly sent it as a new one. The attestor can test this claim by asking the presenting party to go through a proper certificate renewal process where he has to send together his old certificate in order for the new certificate to be signed. Failure to do so will cause the certificate renewal request to be rejected.

If the attestor does not have a copy of the reputable party's certificate in his local certificate repository, the check in step 3 will be passed. The checks in steps 4 to 7 will also be passed if the ill-intentioned party does not have any other identity and the certificate does not have any other signatories. However, the trading software will alert the attestor to verify the validity of the presented certificate by checking with other traders that the party in question is known by his pseudonym, and meeting with the presenting party in person to confirm that his physical appearance is similar to the photograph in the presented certificate. This should reduce the likelihood of a successful attempt by the ill-intentioned party to masquerade as another party.

2) Generate a new key pair and put the public key in a digital certificate using a reputable party's trading pseudonym and his own photograph, and then self-sign the digital certificate with the corresponding private key. In this scenario, if the certificate is sent as a new certificate and the attestor has a copy of that reputable party' certificate locally, the check in step 3 in Figure 5.2 (page 86) will alert the attestor that the trading pseudonym in the presented certificate has been used by another party, as illustrated in Figure 5.3 (page 87). If the presenting party claims that the older certificate is also his certificate and the alert screen shows that his photo appearance in the presented certificate is sufficiently different from the photo in the existing certificate, then there is a genuine doubt whether they are the same person.

If a copy of the certificate of the actual party who is known by that pseudonym is not available in the attestor's local certificate repository, the attestor may not detect such an attempt. This is because all the checks in Figure 5.2 will be successful and the physical meeting with the presenting party will also verify that he is the person in the photo in the presented certificate. However, by checking with other traders about the presenting party's right to use the pseudonym should reduce the likelihood of such an attempt to be successful.

3) Compromise another party's private key and then generate a new certificate that contains the target party's trading pseudonym and his own photograph, and self-sign the new certificate with the compromised private key. The certificate could be passed off as an updated version of the old certificate. However, it is unlikely for such an attempt to be successful because to update or renew a certificate would require a trader to send together his old certificate with the new one to the attestor for verification. If the trader fails to do so, such a request will not be processed by the trading software.

However, if the trader managed to enclose together the old certificate, the checks done by the trading software in Figure 5.9 (page 91) should enable the attestor to detect such an attempt. This can be described in the following scenarios. It is assumed that the attestor has a copy of the old certificate locally.

Scenario 1 - Consider the case where the old certificate in the attestor's local certificate repository is not recorded as "suspected compromised". This may be due to the information about the compromised private key has not yet reached the attestor or the target party does not even know that his private key has been compromised. In such a case, the check in step 4 in Figure 5.9 will be passed. However, if the validity period of that certificate is not within its renewal grace period (for a certificate renewal request), the check in step 5 will be unsuccessful and thus, the new certificate will not be signed. But, if this step is also successful due to the validity period of the old certificate is within the renewal grace period, then the final result that displays the photos in both the new and old certificates should enable the attestor to compare whether they are the same person (Figures 5.11 and 5.12 - page 93). In this case, if the photos are sufficiently different from each other, the presented certificate should not be signed.

Scenario 2 - Consider instead the case where the old certificate in the attestor's local certificate repository is recorded as "suspected compromised". The check in step 4 will alert the attestor that the old certificate is suspected to have been compromised and thus, the presented certificate should not be signed. In addition to that, the attestor can also compare the photos in both the presented and old certificates by viewing the details of each certificate. If the photos are sufficiently different from

each other, then it will be a ground for suspecting that the presenting party may be attempting to spoof the target party's identity.

If a copy of the old certificate is not available locally, the attestor is expected to check with other traders about the presenting party's right to use the pseudonym and also have a physical meeting with him to verify his physical appearance. This should reduce the likelihood of such an attempt to be successful.

5.6.1.2 Compromising The Authentication Process

With respect to the authentication process, there is the risk that although a trader was correctly identified based on legitimate identity credentials, the digital certificate used to link that trader to their identity credentials might be compromised, thereby allowing an ill-intentioned party to successfully complete the authentication process and steal that trader's identity.

One way for an ill-intentioned party to compromise the authentication process is by obtaining the target party's private key. Once the ill-intentioned party has obtained the private key, he can compromise the target party's digital certificate by making signatures using the compromised private key. The ill-intentioned party can, for example;

1) Alter the identity credentials of the compromised digital certificate, for example, substitute the real owner's photograph with his own photograph and pose as the compromised trader by presenting the compromised certificate to deceive others into participating in a trading with him or sending other important information to him, which could possibly cause great damage to the parties involved. In this case, such an attempt should be detected by the trading software checks if a copy of the target party's certificate is available in the relying party's local certificate repository and the theft of the private key is known about. The trading software check in step 5 in Figure 5.13 (page 97) will alert the recipient that the presented certificate is suspected to have been compromised and should no longer be trusted. If there is no record about the theft of the private key, the result of the check will show the photos of the certificate's owner that are sufficiently different from one another, as illustrated in Figure 5.16 (page 100). This should enable the recipient to detect that they are not the same person.

If the target party's certificate is not available locally and the presenting party does not have any other identity or his other identity's certificate is not available locally, such an attempt may not be detected by the trading software checks. However, the trading software will alert the relying party that he is interacting with an unknown party and thus, further actions are expected, such as checking with other traders

whether the subject is known by his pseudonym and meeting him in person to verify his physical appearance. This should reduce the likelihood of a successful attempt.

2) Use the compromised private key and certificate to attest his associates' false identity. In this situation, the relying parties may mistakenly accept the false certificate, as it seems to be attested by a trusted key signer. However, if a copy of the target party's certificate is available locally, the presented certificate's trading pseudonym does not match with any existing certificate and the theft of the private key is known about, the software check in step 3 in Figure 5.17 (page 101) will alert the relying party that one of the certificates of the presented certificate's signatories is recorded as "suspected compromised" and thus, the relying party should exercise caution before relying on the presented certificate. If the theft of the private key is not known about and all the signatories' certificates are within their validity period, the result of the authentication checks will alert the relying party that he is interacting with an unknown party as illustrated in Figure 5.21 (page 103) and thus, further actions are expected to verify the validity of the presented certificate by checking around about its owner's right to use the pseudonym and having a physical meeting with him to confirm his physical appearance.

If a copy of the target party's certificate is not available locally, and the presenting party does not have any other identity or his other identity's certificate is not available locally then the software checks in Figure 5.17 will be successful. In this case, the trading software will alert the relying party that he has never interacted with the presenting party and the certificate's signatories before. Thus, the relying party is expected to check with other traders about the presenting party's right to use the pseudonym and meeting with him in person. This should reduce the likelihood for such an attempt by the presenting party to use a fake identity to be successful.

Another way for an ill-intentioned party to compromise the authentication process is by colluding with his associates to attest his digital certificate that is generated using another party's identity credentials. However, such an attempt should be detected if the relying parties take note on all the alerts given by the trading software in each step in the authentication process. This can be described in the following scenarios:

1) The certificate is generated using another party's trading pseudonym and photograph and is self-signed using the ill-intentioned party's private key. In this scenario, if the recipient has a copy of the certificate of the actual party who is known by that pseudonym in his local certificate repository, the check in step 4 in Figure 5.13 will not be successful and the recipient is expected to perform further checks as discussed in Section 5.5.3.2(A).

However, if a copy of the actual party's certificate is not available locally, the check in step 3 in Figure 5.13 will be passed. The check in step 1 in Figure 5.17 will also be

passed if no photo of another identity in the local certificate repository is found to be similar to the photo in the presented certificate. The check in step 2 in the same figure will alert the recipient that he has never interacted with the presenting party and the parties who have attested his certificate before, if none of those parties' certificates is available in the local certificate repository. In this case, the recipient is expected to verify the validity of the presented certificate by checking with other traders about its owner's right to use the pseudonym and having a physical meeting with the presenting party to verify his physical appearance. This should enable the recipient to detect the presenting party's attempt to masquerade as another party.

If one or more of the signatories' certificates are available locally, the check in step 2 in Figure 5.17 will be passed. The checks in steps 3 to 4 will also be passed if those signatories' certificates are not recorded as "suspected compromised" and within their validity period when the presented certificate was attested. However, the system will alert the recipient that he has never interacted with the presenting party before. Thus, the recipient would be expected to verify the validity of the presented certificate by checking with other traders about its owner's right to use the pseudonym and meeting the presenting party in person to verify his physical appearance. This should reduce the likelihood of a successful attempt by the ill-intentioned party to spoof another party's identity.

2) The certificate is generated using another party's trading pseudonym and the ill-intentioned party's photograph, and is self-signed using the ill-intentioned party's private key. In this scenario, if a copy of the actual party who is known by that pseudonym is available locally, the check in step 4 in Figure 5.13 will not be passed and the trading software will alert the recipient to perform further checks, as illustrated in Figure 5.14 (page 98). When the recipient performs the further check by comparing the photos in both certificates, he should be able to see that they are not the same person.

If a copy of the actual party's certificate is not available locally, the result would be similar to what have been discussed in the first scenario.

3) The certificate is self-signed using a compromised private key and consists of the target party's trading pseudonym and the photograph of the ill-intentioned party. In this scenario, if a copy of the target party's certificate is available in the recipient's local certificate repository and the theft of the private key is known about, the check in step 5 in Figure 5.13 will alert the recipient that the presented certificate is suspected to have been compromised. Thus, the presented certificate should no longer be trusted.

If the target party's certificate is available locally but the the theft of the private key is not known about, the result of this check will display the photos of the certificate's

owner that are sufficiently different from one another, as illustrated in Figure 5.16 (page 100). This should enable the recipient to detect that they are not the same person.

If a copy of the target party's certificate is not available locally, then the result would be similar to what have been discussed in the first scenario.

5.6.2 Addressing Sybil Attacks

As traders in an ad hoc m-commerce trading system are allowed to create their own digital certificates, an ill-intentioned trader may take this opportunity to create multiple identities by creating several self-signed digital certificates. The certificates may consist of different trading pseudonyms and photographs of the user in different disguises. The ill-intentioned trader may then request other traders or his associates to vouch for the certificates' validity.

5.6.2.1 Certificate Attestation by Traders

In this case, if the attestors have a copy of the certificates for the other identities locally and each of the certificates consists of a photograph that has some resemblance to one another, the checks done by the trading software in step 4 in Figure 5.2 (page 86) will be able to detect the existence of several certificates that have similar photo appearances. It will alert the attestor that the photo in the presented certificate is found to have some resemblance to the photo of other identity in the local certificate repository, as illustrated in Figure 5.6 (page 88), and thus further checks on that certificate are required, as discussed in Scenario 1 in Section 5.5.3.1(C). If each of the certificates consists of a photograph that is sufficiently different from one another, then the checks in step 4 will be passed. The check in step 5 also be passed if the certificate's current date and time is within its validity period. However, the result of the checks will alert the attestor to check with other traders about the presenting party's right to use the pseudonym and also meet him in person to verify his physical appearance before signing the presented certificate. This should reduce the likelihood of a successful attempt by the ill-intentioned party to get such an unwarranted endorsement for the presented certificate.

If the attestors do not have a copy of the certificates for the other identities locally, then all the checks in Figure 5.2 will be passed. However, the final result of the checks as illustrated in Figure 5.7 (page 89), will alert the attestors to verify the validity of the certificate by checking with other traders about its owner's right to use the pseudonym and having a physical meeting with him to check whether his

physical appearance is similar to the photo in the certificate. This should reduce the likelihood of such an attempt to be successful.

5.6.2.2 Certificate Attestation by Associates

On the other hand, if the attestors are the ill-intentioned party's associates, then they can attest all of the ill-intentioned party's multiple identities successfully. In this case, if the relying parties have a copy of the certificates for the other identities locally and each of the certificates consists of a photograph that has some resemblance to one another, the trading software checks in step 1 in Figure 5.17 (page 101) will be able to detect such an attempt and alert the relying parties to take the necessary actions, as discussed in this step. If each of the certificates consists of a photograph that is sufficiently different from one another, then the check in step 1 will be passed. However, the check in step 2 will alert the relying parties that they have never interacted with the presenting party and the third parties who have signed the presented certificate before, if a copy of the certificate for the certificate's signatories is not available locally. Thus, the relying parties are expected to check around that the party in question is known by his pseudonym and meet him in person to verify that his physical appearance is similar to the photo in the certificate. This should reduce the likelihood of a successful attempt by the presenting party to have multiple identities. If one or more of the signatories' certificates are available locally, the checks in steps 3 to 4 will be passed if those signatories' certificates are not recorded as "suspected compromised" and within their validity period when the presented certificate was attested. However, the outcome of step 4 will alert the relying parties that they have never interacted with the same identity before. Thus, necessary actions are expected such as checking with other traders about the presenting party's right to use the pseudonym and having a physical meeting with him to verify that his physical appearance is similar to the photo in the presented certificate.

If the relying parties do not have a copy of the certificates for the other identities and the certificate's signatories locally, the result of step 2 will alert the relying parties to verify the validity of the presented certificate by checking with other traders about its owner's right to use the pseudonym and having a physical meeting with him to check whether his physical appearance is similar to the photo in the certificate.

5.6.3 Addressing Whitewashing

Similar to Sybil Attacks, as traders in an ad hoc m-commerce system are allowed to create their own digital certificates, an ill-intentioned trader may take this op-

portunity to hide his misbehaviour or poor reputation by generating a new digital certificate that consists of a new trading pseudonym and photograph, and is self-signed by a new private key. The ill-intentioned trader may then request other parties or his associates to vouch for the validity of the new certificate. The discussion on how the trading software checks in the attestation and authentication processes help traders to detect such an attempt would be similar to what have been discussed in Sections 5.6.2.1 and 5.6.2.2.

5.7 Discussion

This section discusses the things that a trader in an ad hoc m-commerce trading system should and should not do when dealing with PGP digital certificates. It also discusses the responsibilities of a trader as an attestor or a relying party of a PGP certificate, in order to mitigate the above identity-related threats.

5.7.1 Essential Recommendations When Dealing with Digital Certificates

When dealing with digital certificates, traders of an ad hoc m-commerce are expected to do the following:

1) Update their PGP digital certificates periodically as its identity credentials may no longer be valid after a certain period. For instance, a digital certificate may contain an old photograph that does not resemble the current physical appearance of its owner or the parties who have attested the certificate may no longer be members of that particular trading system and so on.

2) Change the private/public keys on a regular schedule. This will limit the time during which the keys are made available to the attackers, which will diminish the opportunities for the attackers to compromise the keys.

3) Distribute a new public key and notification of a digital certificate revocation to other peers in the trading system as rapidly as possible when a private key is compromised. If a trader ever learns or suspects his private key has been compromised, he should contact all people that he has exchanged his PGP certificate or encrypted messages, warn them of the compromise and instruct them to stop using his public key.

4) If a digital certificate is revoked, include some information about the reason for the certificate being revoked.

5) Distribute a notification of a digital certificate renewal to other traders every time he participates in a trading system around its renewal time so that they can acquire a copy of the new certificate in their local certificate repository.

6) Keep the private key secure in a key store encrypted by a long memorable, hard to guess key. It should not be stored on any machine that the traders do not have physical control over.

5.7.2 Responsibilities as an Attestor

As attestation is a crucial stage in establishing online identity in an ad hoc m-commerce trading system, traders should be aware of the following responsibilities when they vouch for the validity of other traders' digital certificates:

1) Properly and accurately identify the subjects and identity credentials in the presented certificates, which include:

- Collect sufficient information as necessary, through trading software checks, personal knowledge, advice from other trusted parties and a physical meeting with the subject, to perform the validation needed to attest the certificates.
- Ensure that all identity credentials are accurate, based on current valid information that is properly checked, for example, the photograph in the presented certificate must be suitably like the physical appearance of the subject.

2) Do not sign another party's certificate using the private key of a certificate that is already expired, or is suspected or known to have been compromised, or has been revoked.

3) Do not attest certificates that lack clear photographs of the whole face of their subject.

4) Check with other traders about the subject's right to use the trading pseudonym and meet the subject in person to verify the validity of a certificate before signing it, although the checks on their certificates by the trading software did not find any suspicious elements.

In an ad hoc m-commerce trading system, as its traders are usually peers with similar role, no authority higher than a peer can be expected to monitor or control any of its security services, and no party's presence can be guaranteed in any of its live trading context, it is unlikely that any peer would be specially trusted by all other peers to monitor the behaviour of other parties in attesting the validity of a PGP certificate.

Anyone who trust a party as an attestor, will consider any credentials signed by that attestor to be valid to the extend of that trust. The trading software check in Step 2 in Figure 5.17 (page 101) will alert the relying parties to perform the necessary actions if the signer of the certificate is an unknown or untrusted party. Multiple signatories on a certificate will lessen the risk that any one certificate signatory is unknown or untrusted as an attestor. Any attempts by the ill-intentioned parties to compromise the certificate attestation process will expose them to the risk of being excluded from the trading system membership if the information about their misbehaviour are circulated among other traders.

5.7.3 Responsibilities as a Relying Party

Similar to attestation, authentication is also vital in an ad hoc m-commerce trading system in order to prevent an ill-intentioned party from misrepresenting themselves as a legitimate party. Thus, as a relying party of a PGP digital certificate, traders should be aware of the following responsibilities when dealing with unknown parties in the trading system, in order to ensure that they are dealing with the right party.

1) Properly authenticate the trading pseudonym, photograph and also private key in the presented certificate before relying on it, by performing the trading software checks in the authentication process, as well as other further checks as advised in the trading software alert message.

2) Take into account all advice in alert messages from the trading software checks such as to check with other traders about the subject's right to use the trading pseudonym and meet the subject in person, particularly in situations where the traders have never interacted with the subject before.

3) Do not accept certificates that have indistinct photographs.

4) Do not accept a certificate if none of its signatories are regarded as a trusted key signer, although the checks done by the trading software on their certificates did not find any suspicious elements.

5.8 Conclusion

This chapter introduces a novel form of support for identity establishment in an ad hoc m-commerce trading system, based on a PGP web of trust model. The scheme allows traders of an ad hoc m-commerce trading system to establish their online identity in a fully self-organizing manner using a trading pseudonym and a photo-

graph as identity credentials in a PGP certificate. The use of a trading pseudonym and a photograph as a trader's identity credentials, and a P2P attestation in this scheme are offered as an appropriate way to deal with identity establishment in such a dynamic ad hoc trading community, in the absence of a CA.

This chapter also analyzes the means by which the scheme can be compromised by ill-intentioned parties. Thus, in order to mitigate identity-related threats, the validity of a trader's PGP certificate is verified in two verification processes; attestation and authentication. Trading software checks in both processes, as discussed in Section 5.5.3.1 and 5.5.3.2, should enable the traders to detect if there is any attempt by ill-intentioned parties to misrepresent their identity credentials, or be alerted that further checks are required in order to verify the validity of the presented certificate before it can be accepted. In addition to the trading software and further checks in both verification processes, traders should also be aware of their responsibilities when dealing with PGP certificates, either as the signer of the certificates or the relying parties of such certificates.

Chapter 6

A Fully Distributed Reputation System for Ad Hoc M-Commerce

6.1 Introduction

Trust development among traders in an ad hoc m-commerce trading system is vital to mitigate uncertainty and risks involved in transactions. It helps traders decide whether to trade with potential trading partners as well as to gauge the degree of confidence that they should give these parties. One way to facilitate such trust is through use of a reputation system. A reputation system enables traders to share their trading experience such as their recent trading histories with other members of the trading system in order to provide evidence of their good faith.

However, designing a reliable reputation system for ad hoc m-commerce trading systems is challenging as traders cannot be expected to spend lengthy periods of time to obtain their potential trading counterparties' reputation reports. Casual online trading is likely to take place over fairly short periods and not on an extended basis due to unpredictable network connectivity and irregular participation by its members. Traders in this type of online trading will sometimes have to make rapid decisions whether to trade or not with a potential trading counterparty. Delays in making such decisions due to having insufficient reputation information might cause a trader to lose a rare opportunity to trade for a valuable resource or item as he might not be offered the same chance again in the foreseeable future. Another important issue is that ill-intentioned traders might try to subvert the reputation system by compromising the reliability of its reputation reports.

Thus, to be effective in assisting traders make fast and reasonably founded trust decisions, a reputation system for ad hoc m-commerce trading systems must provide high availability and efficient retrieval of relevant reputation information as well as

be robust against the sort of attacks that could compromise the reliability of this information.

This chapter starts by discussing the concept of trust in online trading and considers how reputation information helps online traders to establish trust among themselves in Section 6.2. Section 6.3 discusses three key issues in designing a reputation system for an ad hoc m-commerce trading system, namely reputation information storage, integrity maintenance and reliability assurance. Section 6.4 analyses significant related work. Section 6.5 presents the design of a distributed reputation system for an ad hoc m-commerce trading system that addresses the three key design issues. Section 6.6 presents a security analysis of the proposed reputation system. Several recommendations on things that a trader should do when dealing with reputation information are discussed in Section 6.7 and finally, Section 6.8 concludes this chapter.

6.2 Trust Establishment

To be a viable means to conduct online trading, ad hoc m-commerce must mitigate uncertainty and risks in its transactions. Parkhe in [120], describes uncertainty in online transactions as uncertainty about future transactions and about potential trading partners' behaviour in fulfilling their transaction agreements. These uncertainties create a perception of significant risk that might discourage traders from trading. A trust relationship established between two traders lets them believe that their counterpart is a sufficiently reliable and honest party to trade with and that the downside risks are low enough for them to undertake them.

Thus, this section defines the concept of trust from the perspective of online trading and discusses how reputation information helps facilitate trust development among traders.

6.2.1 Trust

Various views on trust [120],[84],[105],[27],[40],[91] have been offered in numerous papers in the literature. In this thesis, trust will be taken to be evidentially founded belief that one party has about another with respect to their reliability and honesty in carrying out cooperative actions where there are significant risks of loss to the first party. This definition emphasizes three aspects of trust in the context of a transaction namely belief, evidence and associated risks.

A trust relationship is established between two traders when both parties have a belief supported by appropriate evidence that the other party is a reliable and honest party to trade with. Such trust enables the parties to view the downside risks in transactions such as being cheated through non-payment, the traded items not being as described and so on, as acceptable. A reliable trader is a party that can be depended upon to carry out a transaction in an expected way. An honest trader is a party that is truthful in his representations, e.g. does not deceive or give misleading information.

The supporting evidence could include testimonials of a trader's trustworthiness, history of evaluated trades, digital certificates attesting identity and so on. A transaction that is potentially risky becomes acceptable if supporting evidence is sufficient for a trader to believe that his trading counterpart is a reliable and honest trader and the likelihood and impact of downside losses are low enough for that trader to expose himself to those risks.

Risk in a transaction depends on several factors such as the value at stake in a transaction, opportunity costs of the transaction and so on. A transaction can be considered as risky if engaging in it makes traders vulnerable to significant loss, which can be in terms of the following:

The item being traded - Loss can be incurred if a trader does not get what he has paid for or has received items or money in exchange for goods that are found to be less than promised or not as described in the trading agreement.

Trading opportunities - A trader may lose opportunities to trade with other traders on better terms if his trading counterpart, who has agreed to trade with him withdraws from their deal or forces inferior terms on the deal under the threat of withdrawal.

Reputation - Loss of reputation is another way of incurring loss. Engaging in a transaction with an ill-intentioned trader who then provides an unfair negative evaluation after their transaction, could negatively affect a trader's good reputation.

Time and effort - Loss can also be incurred if one party does not turn up after making an agreement to meet up at a certain place to do the exchange. In this case, the significant loss is in terms of the time and effort to get to that place.

6.2.2 Reputation

Reputation is correlated with trust [85]. Trading reputation can be defined as a perception about the trading behaviour of a party based on their past trading be-

haviour, which is derived from personal experience with that party or based on recommendations from other parties in a community [174]. A party's good trading reputation would be built up through its honest, reliable and agreeable behaviour in previous trades. Thus, acquisition of a good reputation can be used as an incentive for the parties to be more trustworthy, because parties that do not behave in a trustworthy way will lose reputation and thus will be less likely to be accepted as partners in future interactions or will only tend to be offered less generous terms of trade.

In online trading, reputation reports to some degree reflect the trustworthiness of a trader. They can be a useful reference in assisting traders making trust decisions. Positive experience with a particular trader can help ease other traders' perceptions of risk and uncertainty when transacting with that same trader. Studies [1],[134] show that a reputation system helps to reduce transaction risks by providing a means for traders to develop trust relationships among themselves based upon their past trading history. It is likely that other traders' trust will increase significantly when a trader is perceived to have a good reputation. This motivates traders to act honestly in each of their transactions to maintain a sufficient reputation to remain active in that marketplace. Furthermore, reputations can encourage traders to maintain a persistent identity to continue to benefit from having established a good reputation.

Thus, supporting and exploiting usage of reputation can be an effective way to encourage cooperation and honesty in ad hoc m-commerce transactions. In addition to that, since a good reputation is valuable, it can be an incentive for traders to maintain the same trading identity and build up and sustain its good reputation.

6.3 Design Issues

In order to enable traders to share trading experience among them, an ad hoc m-commerce trading system requires a reputation system with high availability, efficient retrieval and reliable reputation information. However, due to the nature of an ad hoc wireless network and the characteristics of ad hoc m-commerce, to design such a reputation system raises the following issues:

6.3.1 Storage of the Reputation Information

Reputation information needs to be stored and managed in a reliable way to ensure that it is readily accessible and made available upon request. Thus, an important factor to consider when designing a reputation system is to determine where to store

the reputation information, so that it can be retrieved efficiently and be available when required. In an ad hoc m-commerce trading system, because it lacks a network service infrastructure, is self-organized and has no centralized authority to manage a trader's reputation reports, its reputation system has to be fully distributed. One of the challenges of a distributed reputation system in such a dynamic trading system is to determine the most appropriate location to store reputation reports.

One approach is to store a trader's reputation reports with his trading counterparties who have evaluated their trades with him or created testimonials recommending him. However, this approach requires a trader who is considering transacting with another trader to send reputation requests to as many potential recommenders as possible to elicit such reputation reports. This might generate unacceptable communication delays and could overburden other traders. In addition to that, due to dynamic participation in an ad hoc m-commerce trading system, those third parties may also be unreachable or no longer active in the trading system at the time the reputation reports are required. It also cannot be expected that all traders in the trading system will be willing to use up their mobile device's storage to store other parties' information.

A second approach would be to store all reputation information in a trusted shared store that is always accessible and access it on demand. However, this approach is infeasible in ad hoc networked communities. These communities have no computing components that are omnipresent to host such a store. Nor does it seem viable that such a store could be established in some distributed way across whatever nodes of the community happen to be connected by ad hoc networking at the moment.

A third approach is called a self-maintaining approach where traders store their own reputation reports locally. This approach minimizes communication overhead and delay as it does not require any reputation request to be sent to any other third parties and the requested party does not need to wait for recommendations from others. It will also make the retrieval of reputation information more efficient as it is stored locally and can be provided anytime by its owner when requested by others. Furthermore, it makes it possible for traders to get a detailed view of his potential trading counterparty's trading history.

6.3.2 Integrity of the Reputation Information

The integrity of reputation information is an important element that is directly connected with the reliability of a reputation system. In an ad hoc m-commerce trading system, there are several ways in which ill-intentioned parties can try to compromise the integrity of reputation information. One of the most obvious ways would be to

intercept or alter other parties' reputation information during its transmission over an insecure ad hoc wireless network. Another possible way is to alter their own reputation information while it is being stored on their mobile device. Thus, transmitting and storing such information should be done in a secure manner in order to ensure its integrity.

6.3.3 Reliability of the Reputation Information

The usefulness of a reputation system depends critically on the reliability of its reputation information. Unreliable reputation information will expose traders to the risk of significant loss if it incorrectly supports a good reputation for a dishonest trader. In an ad hoc m-commerce trading system, ill-intentioned traders might try to compromise the reliability of such reputation information by providing unfair deal evaluations (overstating or slandering) or by colluding with their accomplices, either to increase their own reputation (hyping) or harm other parties' good reputation (bad mouthing). Another way an ill-intentioned trader can try to manipulate reputation information is by creating and using multiple identities (Sybil Attack) to create many bogus deal evaluations. For example, a trader creates multiple trading pseudonyms and corresponding credentials to enable him to create bogus transactions with those identities. He then uses those identities to provide good evaluations for each of the transactions that he has created, so that his own reputation will apparently be increased.

Thus, to ensure traders obtain reliable reputation information, a reputation system for an ad hoc m-commerce needs to be robust against Sybil Attacks and misbehaviour-related threats such as unfair deal evaluations and collusions.

6.4 Related work

The emergence of online trading communities has changed many aspects of conducting business and demands corresponding means for trust development among participating parties in such a community to minimize transaction risks. A considerable amount of research has been conducted into this issue and a number of solutions have been proposed in the literature [172],[86],[8],[51],[176],[104].

Xiong and Liu in [172] have proposed a dynamic trust model for P2P e-commerce communities using a transaction-based feedback system where a trader's trustworthiness is measured based on five factors, namely satisfaction, number of transactions, credibility of feedback, transaction context and community context. It is a fully de-

centralized system that uses an overlay for supporting trust propagation and a public key infrastructure for securing remote trust scores. This proposal is among the most credible yet for supporting decentralized support for P2P online transactions that require trust judgements. However, the assumption made in the proposal that network connectivity is always available for traders to obtain reputation information seems to be unlikely to be fulfilled in ad hoc m-commerce trading communities. This proposal also assumes that a reputable party will provide accurate deal appraisals, which may not always happen.

Jurca and Faltings in [86] have proposed an incentive-compatible mechanism using a side-payment scheme to encourage agents to report reputation information accurately. The side-payment scheme is organized through a set of agents that act as brokers to buy and sell reputation information. These broker agents are called R-agents. Agents can buy another agent's reputation information from an R-agent at a certain cost F_1 and then sell reputation information to the same R-agent at another cost F_2. The integrity of reputation information and its binding to its owner is protected using a cryptography mechanism. However, this approach is vulnerable to collusions even when only two agents are involved. Any agent can collude with an R-agent to provide fake reputation information to other agents. Furthermore, it is not useful for trading parties in ad hoc m-commerce trading systems to store their reputation information with a third party as the availability of such reputation information cannot be guaranteed every time it is required. This is because the party who stores the reputation information may not be participating in the trading system during the transaction period or may no longer be an active participant. It will take unpredictable periods of time for the requestor of the reputation information to get in contact with that party.

Another approach by Aberer and Despotovic [8] is based on a binary valued concept of trust, where an agent can only be trustworthy or not. In their approach, only information on dishonest transactions is used to evaluate the trustworthiness of each agent. If an agent discovers that its counterpart is dishonest in their transaction, that agent can forward a complaint about its counterpart's misbehaviour to other agents. To store the complaints in a P2P network, a decentralized storage method, called a P-Grid is used. To evaluate the trustworthiness of a particular agent, an agent will search the leaf level of the P-Grid for complaints on that agent. The main interest in this approach is that it does not require any centralised infrastructure for agents to assess the trustworthiness of other agents as well as to store complaints on each agent's misconduct. However, the use of complaints as the only relevant data to assess trustworthiness is not an adequate way of evaluating an agents reputation. The absence of complaints is not positive evidence of an established reputation. Only a reasonable number of recently conducted mutually satisfactory trades is evidence

of that. In addition to that, in Aberer and Despotovics approach, no consideration is made of the possibility of an agent making an inaccurate complaint. It is important to consider this issue to ensure that there is little likelihood of a malicious agent undermining the purpose of the reputation system by compromising the reliability of a complaint.

6.5 Design

This section presents the design of a distributed reputation system that aims at providing an effective way to facilitate trust development among traders in an ad hoc m-commerce trading system by addressing the three key design issues discussed in Section 6.3, namely reputation information storage, integrity maintenance and reliability assurance. To enable efficient retrieval as well as a high availability of reputation information, it is proposed that the reputation system for ad hoc m-commerce trading systems let traders maintain their own reputation information locally and share their knowledge about other traders' trading behavior in a totally P2P manner without having to rely on network services that are always available. It is also proposed that a sanction-backed mechanism be employed to encourage traders to provide truthful reputation reports in order to ensure the reliability of such information.

6.5.1 Reputation Information

In many existing reputation systems, traders build their reputation by means of deal evaluations which are provided after the completion of each transaction that they participate in. Positive evaluations can be used as proof that a trader has engaged in transactions before in a proper manner whereas negative evaluations are evidence that a trader has misbehaved or at least failed to satisfy in his previous transaction agreements. To help traders make sensible trust decisions, the proposed reputation system for ad hoc m-commerce uses both positive and negative evaluations.

However, the use of deal evaluations as the only relevant reputation information to evaluate a trader's trustworthiness will make it difficult for new members in a particular trading system to begin participating in transactions. They will struggle to get started as they can only build a reputation after they have participated in several transactions. A testimonial recommending that a trader is worth dealing with from a respected member of the forum could help them get started. Testimonials provide a secondary method for a trader's good faith and professionalism to be supported. Their worth depends on trusting the judgement of their provider and

their provider's own reputation is a good basis for deciding on that.

6.5.1.1 Deal Evaluation

In an ad hoc m-commerce trading system, traders are expected to generate a deal evaluation of their counterparty's trading conduct after the completion of each transaction, digitally sign it and then send it to their trading counterparties. This will enable the traders to store reputation information about their trading conduct on their mobile device, which will make such information readily accessible when it is required in their future transactions. A deal evaluation that is signed by its sender's digital signature before it is sent to its recipient will ensure that no other third party can alter it during transmission without the knowledge of both its sender and receiver. Any attempts by the recipient to modify it when it is stored on his mobile device will also be detectable. Thus its authenticity and integrity can be guaranteed. To prevent both parties from repudiating offers or bargain struck between them, the deal evaluation will also contain a transaction contract that is digitally signed by them [118] as a proof that they have agreed to engage in the transaction.

There are many ways in which traders can evaluate their trading counterpart's behavior in satisfying their trade.

1. A rather simple one would use a one dimensional evaluation parameter where 1 is used to indicate a good transaction, -1 to indicate a bad transaction and 0 to indicate neutral, as is used in eBay's reputation system. This approach, although simple to understand, is too unspecific and does not allow traders to clearly specify the variations in the quality of the items being traded or the quality of the behaviour of a trader in fulfilling their transaction agreement. A reputation system with such a common or subjective evaluation parameter would blur pertinent detail into a rating that merely gives an overall impression, which could subsequently lead to illfounded trust decisions.

2. A second approach adopted by some existing reputation systems evaluates trades by means of a rating using a single numerical value. For example, trader A gives a value 0.9 to trader B for satisfying their transaction agreement on a scale of 0 (bad) to 1 (good). However, single numerical measures like this misleadingly suggest that one dimension of valuation sums up all the key qualities at stake to quite a fine degree of precision.

3. A third approach is to use a scheme that differentiates out different quality aspects based on several parameters such as:

- **Honesty in describing what is traded** - This expresses a trader's satisfaction as to the quality of the traded items being as described.
- **Conformity to agreement** - This expresses a trader's satisfaction with how well the other party has fulfilled the transaction agreement, e.g. made payment or delivered the traded items as agreed.
- **Manner of dealing** - This expresses a trader's satisfaction with how well the other party behaved in doing the deal. Did they act in good faith or did they try to take unfair advantage or cheat.

To express the amount of satisfaction for each parameter, a 4-category grading scheme as shown in Table 6.1 might be used to signify fully satisfied, satisfied, unsatisfied or wholly unsatisfied. Traders can also qualify their satisfaction by leaving short textual comments.

Rating	**Honesty**	**Contractual Compliance**	**Manner**
Fully Satisfied	Traded items exactly as described	Fulfilled their end exactly	Behaved well
Satisfied	Traded items roughly as described	A bit late or not quite as agreed	Grudging but roughly acceptable
Unsatisfied	Traded items barely as described	Late payment or delivery	Tried to take unfair advantage or failed to deal fairly
Wholly Unsatisfied	Traded items not at all as described	Non-payment or non-delivery	Cheated or tried to cheat

Table 6.1: Possible grading scheme in a deal evaluation

Consider for example, a scenario where trader A has bought a second hand bike from trader B in a selling or buying items trading forum. Trader B describes the bike as new and never been used but when trader A goes to collect the bike and pay for it, it is not exactly as described but is still in an acceptable condition. After the trade is completed, trader A might give the following evaluation to trader B, as shown in Table 6.2.

Trader: SmartJane **Item Traded:** Bicycle **Date:** 19 September 2013			
Honesty	**Contractual Compliance**	**Manner**	**Comments**
Satisfied	Fully Satisfied	Fully Satisfied	Not brand new but in good condition and barely used

Table 6.2: Example of a deal evaluation

To aggregate such evaluations data, a simple summation scheme might be used by a trading software to total up the number of reliable ratings received by a trader for each parameter. For example, a trader with 10 recent transactions in the past 6 months might have the following deal evaluations summary as depicted in Table 6.3.

Deal Evaluation Summary: Last 6 months Total Transactions: 10			
Rating	**Honesty**	**Contractual Compliance**	**Manner**
Fully Satisfied	5	2	0
Satisfied	3	6	8
Unsatisfied	2	1	2
Wholly Unsatisfied	0	1	0

Table 6.3: Example of a deal evaluation summary

The third approach seems to be more suitable for an ad hoc m-commerce trading system as it enables the evaluation given by different parties to be comparable using several categories of degree as well as being simple for traders to understand and make fast trust decisions. Flea market traders using an ad hoc m-commerce application for low value trading might not be keen to use a more complex evaluation scheme as it might require them to spend a lengthy period of time in order to understand how it functions. If the traders fail to understand properly how the evaluation scheme works, there is a possibility that they might unintentionally give inappropriate or inaccurate evaluations to their trading partners. In addition to that, a reputation system with complex evaluation parameters would require participants to spend substantial amounts of time grading deals on all these parameters. Busy traders with no big ticket risks might be tempted to skip doing this thoroughly which could lead to incomplete or illconsidered evaluations that undermined its value.

However, as this thesis only focuses on addressing three key design issues as discussed in Section 6.3, the suggested scheme for evaluating deals is not presented as preferable to use over any other scheme of evaluation. The key point is that whatever scheme is used to evaluate deals, it should clearly distinguish good from bad evaluations to suitable degrees so that software can summarize such data in a readily understood form. It should also suit the type of trading involved so that capturing deal evaluations after every trade or attempted trade is realistic to expect will happen.

Ad hoc m-commerce trading forums might be expected to design their own deal evaluation templates to suit the stakes involved in trading, the manner in which exchanges take place and the norms of acceptable conduct in such trading.

6.5.1.2 Testimonials

One way for traders to share their expressions of trust about a particular trader's honesty in performing transactions is by providing tradeworthiness recommendations in the form of a testimonial. Testimonials from respected and well known reputable traders can be an effective means for new comers in an ad hoc m-commerce trading system to build trust with future trading partners, which will then help them to get started and quickly participate actively in the trading system's activities. Recommendations of this kind would also help established traders be accepted as reputable in addition to favorable evaluations of their past deals. Testimonials have value as well in helping traders who have been unsatisfactorily evaluated in a few deals to have these evaluations put in a wider perspective of relevant evidence.

One approach to capture such tradeworthiness recommendations in an ad hoc m-commerce trading system is to use the testimonial template as shown in Figure 6.1. Its structure helps elicit key aspects and makes comparisons easier to make. An alternative would be to use unstructured text of a certain maximum size. Either might be employed, or an ad hoc m-commerce trading forum might design their own testimonial template to reflect the norms and forms of the style of trading accomplished within.

Figure 6.1: Testimonial template

To ensure that a testimonial is authentic and not a fake recommendation by an ill-intentioned party, it needs to be digitally signed by its sender before it is sent to its recipient.

6.5.2 Reputation Information Storage

As discussed in Section 6.3.1, the most appropriate and reliable way to store and manage reputation information in an ad hoc m-commerce trading system is to allow traders to maintain their own reputation information in their mobile device local repository. The benefits of allowing traders to store their own reputation information locally are;

- The retrieval of such information will be more efficient as it can be accessed immediately by its owner when requested by others without having to rely on any third parties to supply it. This reduces communication overheads among traders.
- It addresses the availability issue for much of the reputation information. If such information is stored on any other third party's mobile device, it might not be available when it is required because that third party may not be available or no longer participate in the trading system.
- It simplifies the storage issue in an ad hoc m-commerce trading system and also reduces each trader's storage overheads.

However, if traders store their own reputation information locally, two issues need to be addressed. The first issue is the integrity of the reputation information as ill-intentioned traders might attempt to alter it while it is in their local repository in order to increase their reputation dishonestly. The other issue is that traders may refuse to supply or fail even to store negative evaluations about themselves.

For the first issue, it will be difficult for the ill-intentioned traders to tamper with the reputation information in their local repository without being detected by other

traders who receive their reputation reports. This is because these reports will be signed and so long as a checker has access to the public key in the signer's public key certificate, the checker will be able to detect any changes made to the document after it is signed and thus its authenticity and integrity will be guaranteed. It will also ensure that the evaluator cannot credibly deny having made that deal evaluation or testimonial.

To guard against traders discarding or withholding poor evaluations of their trades, traders are expected to multicast markedly poor evaluations of trades within the trading community. Recipients would be expected to store such data but could condense or expire it as it ages or threatens to exceed allocated storage space. It is also recommended that trading software implementing this approach provide no software supported means for users to discard or filter out unwanted recent evaluations of their dealing behaviour when sharing evaluation data. This would make it difficult for all but the most technically sophisticated to selectively edit the presentation of their trading history.

6.5.3 Sanction-backed Mechanism

A sanction-backed mechanism is potentially useful in handling misbehaviour among traders. One example type of misbehaviour in online trading is where a buyer pays the seller for an item but the seller does not transfer the traded item at all to the buyer, or transfers an item to the buyer that is not as described or promised in their deal agreement or has undisclosed quality deficiencies. In this case, if the seller is not sanctioned after receiving a series of poor deal evaluations from his trading counterparts due to his misbehaviour in several transactions, then he has no incentive beyond a poor reputation to behave properly and honestly in all of his transactions. This will subsequently affect other traders' confidence to participate in such trading system as there could be perceived to be insufficient disincentive to constrain traders from misbehaving or cheating in their transactions. Thus, it can be useful to employ a sanction mechanism in an ad hoc m-commerce trading system as an inducement to encourage traders to behave in a proper manner and comply with the rules and regulations of the trading system, especially when participating in a deal, or providing deal evaluations or testimonials to other traders, or attesting other traders' credentials. A sanction-backed mechanism can also be an effective way to restrict an ad hoc m-commerce trading system's membership to only parties that are regarded as reasonably trustworthy by other participating parties.

Without a centralized authority and established network infrastructure, it can be a challenging task to administer sanctions in an ad hoc m-commerce trading system. The mechanism needs to be distributed and controlled by the traders themselves

in a fully P2P manner. This thesis advocates using exclusion from membership of a trading forum to sanction traders that misbehave or have a series of poor deal evaluations. This mechanism enables any trader who has evidence about a particular trader's misbehavior to multicast a proposal to exclude that trader from a trading forum's membership to other traders in the trading forum. The exclusion proposal will consist of the target party's trading pseudonym, brief reasons for the exclusion, relevant evidence and also the digital signature of the party who makes the proposal [118]. To reduce the risk of traders being unfairly excluded from a particular trading forum's membership, traders are expected to verify the identity of the sender of the proposal exclusion is whom he claims to be by checking his PGP certificate through the certificate authentication process and check his credibility, whether poor evaluation reports have been broadcast about him or whether he himself is the subject of an exclusion proposal. As the decision for the exclusion will be based on collective decision making by any sufficiently large number of current forum members, depending on each trading forum's exclusion policy [118], traders with views on the proposal will have the opportunity to give their vote. If they do not regard the sender of the exclusion proposal as a credible party, they can vote their disapproval. Having a vote based exclusion policy helps diminish the possibility of unfair exclusions due to collusion among ill-intentioned traders as they would need to have a substantial number of associates in order to obtain a quorate decision for the exclusion. The sender's digital signature on the exclusion proposal will ensure that he is accountable for any exclusion proposal that he has made. Any unfair exclusion proposal can be used as an evidence for other traders to exclude him in turn from a trading forum's membership for his misbehavior. More details about the exclusion mechanism will be discussed in Chapter 7.

Thus, a trader who makes a habit of providing unfair negative evaluations or colluding with accomplices to harm other traders' reputations or unfairly tries to exclude them, will also be open to the risk of being excluded from membership of a trading forum if other traders receive poor reputation reports and an exclusion proposal from one of his unsatisfied trading counterparties. As mentioned in Section 6.5.1.2 above, testimonials from respected reputable traders in the trading forum can be valuable evidence to rebut a trader's poor evaluation report if they can be obtained. The sanction mechanism will be a significant incentive for traders to desist from behavior that creates negative evidence that other traders can use as a basis for excluding them from a trading forum's membership. The proposed identity support scheme as discussed in Chapter 5 will also make it difficult for them to reenter with a whitewashed new identity once they are excluded.

6.6 Security Analysis

Misbehaviour by ill-intentioned traders is a major threat to the effective operation of an online trading system. The existence of such traders may subvert the reliability of a reputation system and the functionality of a trading system, which will subsequently cause loss of trust among traders if the system fails to detect them in a timely way and constrain their misbehaviour effectively. Generally, ill-intentioned traders can do such damage by working alone or in coalitions, such as by behaving dishonestly in their transactions or manipulating reputation information through collusion with associates or multiple identities in order to gain personal benefits, and so on.

Thus, this section examines the means by which the ill-intentioned parties in an ad hoc m-commerce trading system can pose threats to compromise the reliability of its reputation system and discusses how the proposed design of a reputation system can detect and mitigate such threats to a sufficient degree.

6.6.1 Mitigating Poor Trading Behaviour

In an ad hoc m-commerce trading system, traders can act dishonestly in their transactions in many ways, which include the following:

- Provide misleading information to their trading partners about the items to be traded in terms of their price, quality, originality, condition and so on. For instance, a seller can advertise a used computer as a brand new one, or a fake designer watch as a genuine one.
- Deceive in their transactions. For instance, a seller does not provide the item that has been traded to the buyer or a buyer does not pay the seller for the item that has been traded between them and so on.

To mitigate such poor trading behaviour in an ad hoc m-commerce trading system, traders are encouraged to multicast negative evaluations about a particular dishonest trader to the whole community of the trading system. By sharing such negative trading experience with other members of the trading system, the opportunities for the dishonest trader to participate in future transactions, especially the profitable ones are likely to be reduced. This is because when negative information about a trader is spread over the whole community, the other members who receive such information may refuse to deal with that trader to avoid from being exposed to significant risks of loss. Negative evaluations that a trader receives, even from a

single transaction are likely to damage that trader's reputation, which will significantly diminish the other traders' confidence and trust to engage in a deal with that trader. Thus, the sharing of negative trading experience among members of a trading system helps to motivate traders to behave and fulfill each of their transactions honestly as the gain that they obtained from their misbehaviour might be smaller if compared to their future losses due to their poor trading history.

In addition to the sharing of negative trading experience among traders, a trader that receives a series of negative evaluations from his trading counterparts is open to the risk of being excluded from membership of the trading system. An exclusion mechanism is used as a means to encourage cooperative behaviour among traders in an ad hoc m-commerce trading system by inflicting indirect punishment on the users who cheat or misbehave. Such a mechanism can assist in the establishment of trust among traders in such an ad hoc trading community by excluding traders that misbehave or have a history of poorly evaluated trading deals.

However, the sharing of negative evaluations among traders might create another risk for an ad hoc m-commerce trading system. An ill-intentioned trader might provide unfair negative evaluations about an honest trader with the intention of damaging that trader's reputation, through either slandering or badmouthing. The issues of slandering or badmouthing in an ad hoc m-commerce trading system are addressed using testimonials and an exclusion mechanism. As discussed in Section 6.5.1.2, testimonials from trusted and well known reputable traders in the trading community can be used as relevant evidence to support a trader's explanation to other members that he has been evaluated unfairly by his trading counterpart(s). Another way to address the issues of slandering and badmouthing is to use an exclusion mechanism to sanction traders who provide unusually high numbers of negative evaluations. In this case, a trader can also include his testimonials as evidence to support his exclusion proposal to exclude ill-intentioned traders that have given him unfair negative evaluations from a trading system's membership.

6.6.2 Mitigating Overstating and Hyping

The issue of overstating and hyping is challenging to tackle. It requires a mechanism that provides significant incentives for traders to remain honest under any circumstances. Overstating and hyping are not necessarily harmful. They are only so if traders use artificially boosted reputations to defraud others. To boost their reputation through overstating or hyping, ill-intentioned traders may cooperate with their associates or use multiple identities to create bogus transactions and so provide good evaluations for those transactions. For this reason, it is important for traders when considering deal evaluations to take into account who they are from. If the

evaluations are from known cronies of a dubious trader, then they can be accorded little weight however ecstatic they are. If they are from completely unknown parties with no other known participation in trading with parties the assessor is familiar with, then they should equally be accorded little weight. Only evaluations from parties the assessor has favorable knowledge of either directly or indirectly can be accorded credence.

Traders can also be provided with a means to verify the authenticity of a transaction. This can be achieved by requiring participants to produce a transaction contract after both parties have agreed to engage in a deal. A trader needs to send the transaction contract that has been time stamped and digitally signed by both parties together with a deal evaluation to his trading counterpart after the completion of each transaction as a proof that the transaction is real and has occurred between them.

6.6.3 Mitigating Sybil Collusions

Sybil collusion is a major collusion hazard that can occur in any reputation systems that has weak identification processes. Ill-intentioned traders in a trading community may exploit weak identification processes to generate multiple new identities. A study has shown that a user can then use these identities to collude to boost his own reputation or his associates' or damage another trader's reputation [96], which may subsequently lead other members of the trading system to making inaccurate trust decisions. In order to prevent sybil collusions, a trading system needs to provide a means to constrain a trader from generating and also exploiting multiple identities, which can be achieved through the following approaches:

- Restrict the generation of multiple identities in the identity establishment process.
- Detect the presence of multiple identities within the identity verification processes.

In an ad hoc m-commerce trading system, it might be difficult to restrict the generation of multiple identities as ill-intentioned traders might compromise the digital certificates generation process in Section 5.5.2. This is due to the fact that traders are allowed to create their own self-signed digital certificates and there is no centralize authority or a CA to control such process. Thus, the only way to mitigate sybil collusions is by detecting the presence of sybils through digital certificates verification processes, which include the attestation and authentication processes as discussed in Section 5.6.2. The use of a photograph in a trader's PGP certificate

will make it difficult for traders to operate with multiple identities without this becoming apparent [119].

6.7 Discussion

This section discusses the things that a trader in an ad hoc m-commerce trading system should do when dealing with reputation reports or testimonials in order to mitigate misbehaviour-related threats. Before relying on any reputation reports or testimonials from other traders, traders of an ad hoc m-commerce are expected to do the following:

1) Perform a trading software check to ensure that nothing has changed since the last digital signature was applied to any of the deal evaluations in the reputation report or the testimonials. This is to ensure that the integrity of such documents has not been compromised when it is stored in its owner's local repository or during transmission.

2) Verify the validity of the digital certificate of each party that provides the deal evaluations or testimonials to ensure that there is no sybil collusion attempt.

3) Check the credibility of the trader who sends a negative evaluation whether poor evaluation reports have been broadcast about him or whether he himself is the subject of an exclusion proposal.

4) Check the membership status of the parties that provide the deal evaluations or testimonials to ensure that they are not recorded as being excluded from membership or a subject of an exclusion proposal in their local membership list.

6.8 Conclusion

This chapter has discussed three key design considerations in implementing a fully distributed reputation system that can provide effective ways to facilitate trust development among traders in ad hoc m-commerce trading systems, namely reputation information storage, integrity maintenance and reliability assurance. It also has presented the approach to address the three key design issues in order to assist traders in making faster and more reliable trust decisions.

To enable efficient retrieval and high availability of reputation information, the proposed approach lets traders maintain their own reputation information locally and share their knowledge about other traders' trading behavior in a totally P2P manner

without having to rely on network services that are always available. It advocates reinforcing this with a sanction-backed mechanism that lets traders collaborate to exclude any member that has misbehaved unreasonably or has an overly poor trading history from a trading system's membership to encourage traders to provide truthful reputation reports.

This chapter also has examined the means by which the ill-intentioned traders in an ad hoc m-commerce trading system can pose threats to subvert the reliability of its reputation system and discussed how the proposed design of a reputation system can detect and mitigate such threats to a sufficient degree. With support from the proposed group membership service [118] and identity support scheme [119], the aim is that this type of reputation system will make ad hoc m-commerce a viable means to conduct online trading via ad hoc networking.

Chapter 7

Collaborative Group Membership in Ad Hoc Communities

7.1 Introduction

A basic concept in ad hoc m-commerce trading systems is the formation of a trading forum by two or more peers that are in the vicinity of each other and run an appropriate software application. This trading forum defines the rules of trading and provides the context for mobile users to engage in mobile commerce using ad hoc wireless networking [117]. Its participants communicate and cooperate with each other by utilizing their local resources and also their neighbours to accomplish their transactions and other related activities. As an example, a group of peers with wireless networking capability and a mobile auction application installed on each device comes into communication range with each other. One of the peers reestablishes a trading forum that offers auction services and advertises it for other peers with similar interests to join. Peers able to join the trading forum session can then participate in the auction activities as sellers or bidders. The mobile auction application that runs on each peer's device handles all the auction processes and provides a graphical interface to the users. After the completion of each transaction, peers can provide deal evaluations to each other.

A trading forum can be open to all comers or it can choose to use membership to separate the members from the outsiders. Group membership can be the first step towards creating a more secure and trusted environment for traders to trade and communicate with each other. As new parties apply to join and existing members may have to be excluded, the management and maintenance of such trading forums entails support for a service to handle group membership. The function of a group membership service is to track membership changes in a trading forum and help

determine whether a peer is currently a member of a particular trading forum [22]. It consists of mechanisms for peers to join and be excluded from the trading forum, as well as to verify membership.

However, managing group membership in an ad hoc m-commerce trading forum is a challenging task as peers may only have partial knowledge of the current membership due to frequent network disconnections, infrequent participation and delays in communication via intermediaries among them. The absence of a centralized network infrastructure adds more complexity to this problem. Thus, this chapter presents a fully distributed and self-organizing approach to managing group membership in such a loose ad hoc m-commerce trading community. It is designed to suit the dynamic nature of ad hoc wireless networking and the social characteristics of ad hoc m-commerce.

The rest of this chapter is organized as follows. Section 7.2 discusses how the group membership acts as a filter to constrain trading parties' participation into an ad hoc m-commerce trading system. Section 7.3 discusses and analyses significant related work. The requirements for managing a group membership for an ad hoc m-commerce trading system are described in Section 7.4. Section 7.5 presents the details of each mechanism in the group membership service for an ad hoc m-commerce trading system, which include a join mechanism, membership renewal mechanism and also exclusion mechanism . Section 7.6 demonstrates a number of reference scenarios. Section 7.7 presents a security analysis of the proposed group membership service. Several recommendations on things that a trader should do when dealing with membership vouchers and also when participating in a group decision making process are discussed in Section 7.8 and and finally, Section 7.9 concludes the chapter.

7.2 Membership is a Filter

In ad hoc m-commerce trading systems, there is no network service provider that can be relied upon to provide security services, or central administration to control or manage its traders and their trading related activities. Its participating parties will utilize their available computing resources to communicate and cooperate with each other in order to participate in m-commerce transactions as well as to control the security settings of such trading systems. This situation is of potential security concern since not all of the participating parties will behave properly all the time and cannot always be trusted in each of their transactions or other related activities that require their participations, especially in controlling the security settings of the trading forum. For instance, the attestation process of a trader's digital certificate

will only be reliable if the parties who vouch for the validity of the certificate are recognized by other members of the trading forum as a trusted party. Thus, it is necessary for ad hoc m-commerce trading systems to have a means to constrain a trading forum's participation to only traders that are regarded as reasonably trustworthy by other members of the forum in order to establish greater trust and more secure interactions among its group members.

Defining who is a member of a particular trading forum can be an effective means to constrain a trading forum's participation, which can be accomplished using group membership. A trading forum membership can be restricted to only parties that trust each other to a reasonable degree. This means that in order to remain as a member of a particular trading forum, each trader needs to behave in a proper manner all the time and have a decent reputation towards every other trader based on their past trading experiences and also the sharing of trust among them. Group membership is thus subject to a trader's behaviour and reputation among the peers in the trading community. A trader that has misbehaved or has a poor reputation might be considered as untrustworthy by other members of the trading forum. They may no longer be prepared to let him remain active in the trading community and as a result exclude him from the trading forum's membership.

Along with a reputation system, trading forum membership is useful to encourage traders to behave honestly and be more responsible in each of their activities. This is because a trader needs to maintain their good behaviour and reputation in order to establish a good relationship with other members of the trading forum. A party who has gained trust and respect from other traders in the trading forum is more likely to get valuable information, better cooperation and responsible behaviour from those traders and thus, is usually less likely to misbehave if he intends to remain active as a reputable and trusted party in such a trading community. Those with no or little reputation need to build their reputation by behaving well and be honest in each of their activities in order to gain respect from other traders of the trading forum and be recognised as a trustworthy party. This will indirectly limit the negative behaviour of the traders.

7.3 Related Work

Several relevant research studies have been done in the area of group membership in ad hoc wireless networks such as [102],[148],[100],[126],[136]. The main focus of most of the work is to provide secure communications among group members. Some of the solutions proposed are based on group key agreements. Maki, Aura and Hietalahi in [102] have proposed a distributed certificate-based system to establish

secure communications among members in ad hoc groups, where a certificate that is signed by a group key is used to indicate the membership of each member. The group key is used as the identifier of the group and is generated by a group leader who is responsible for managing the group membership. To avoid a single point of failure, a group leader's authority is distributed to multiple sub-leaders. Thus, a group can have one or more group leaders or sub-leaders.

A similar approach is used by Steiner, Tsudik and Waidner in [148] to address the issue of secure group communications in dynamic peer groups. They have proposed a protocol called CLIQUES which is based on a multiparty extension of Diffie-Hellman key exchange. In this protocol, all members contribute to the establishment of a group key. Whenever there is a membership change, the group key is reconstructed. This approach also depends on having a group controller to manage the group membership.

Liu, Sacchetti, Sailhan and Issarny [100] in their design of a generic group management service for MANET have also proposed a group leader for managing the group dynamics. In their approach, the group leader's role is rotated from one member to another in order to distribute the load of group management among members and also to address the issue of group leaders dropping out of participation. The selection of the group leader is based on a number of criteria that have been defined.

Another approach is a virtual partitioning (VP) based group membership algorithm by Pradan and Helal [126]. This approach requires each group member to maintain a complete and consistent view of group membership.

Roman, Huang and Hazemi in [136] have also proposed an algorithm to maintain a consistent view of group membership in ad hoc wireless networks based on location information.

Group key agreement does not seem to be workable for ad hoc m-commerce trading forums. Participation by all members on a regular and frequent basis would be required in order that new group keys could be constructed in a timely way for each membership change and also for each member to get access to the new group keys every time they are reconstructed. However, casual local online trading, a representative type of ad hoc m-commerce is likely to involve a mixture of frequent and infrequent participants and quite an amount of irregular participation. Thus, it may not be possible for a new group key to be constructed in a timely way for each membership change on each occasion that requires contribution by all group members. It will take unpredictable periods of time for all members to be available for the reconstruction process to happen. This might delay the first opportunity for a new member to participate in the group communications as well as other activities of the trading forum. This might also give an opportunity for a member subject

to exclusion proceedings to remain as a member for a longer period of time. On other occasions, the unavailability of some members during the reconstruction of the group key might cause them to be excluded and the group shrinking as a subset of the members reconstruct the group key among themselves. The reacceptance of these unavailable members in the trading forum would demand the group key be reconstructed again. This might lead to endless reconstruction of group keys as frequent and regular participation by all group members cannot be guaranteed in ad hoc m-commerce trading forums.

A hierarchical structure where one or more group leaders are responsible for managing the group membership also does not seem to be workable for our work as the presence of such authority in the current group context cannot be guaranteed all the time. Furthermore, the loose nature of relationships in casual local trading networks does not support the assumption of a core of well trusted parties around which the rest of the trading community is constituted. Thus, a flat structure where all members are given equal responsibility to manage the group membership would seem to be more appropriate.

The requirement for each member to maintain a complete and consistent view of current group membership is also not realistic for ad hoc m-commerce trading forums. Communication among members will often involve intermediaries, be subject to frequent disconnections and take unpredictable periods of time from minutes to several days or weeks with infrequent participants. Getting all group members to participate in every membership decision will take too long to be practical. So membership decision making needs to be delegated to subsets of the membership and other members will have to accept their decision making when it is eventually communicated to them. That in turn means that every member will only have a partial view of the membership

7.4 Requirements

Due to the challenges posed by the nature of ad hoc wireless networking and the social characteristics of ad hoc m-commerce [117], the following requirements for managing a trading forum's group membership will be needed on top of the usual requirements for interactive m-commerce software such as adequate quality of service and reliability in the wireless network, end-to-end security and so on:

Resource-limited - The processes and operating costs of group membership management should be affordable for resource-constrained devices.

Dynamic - Group membership management should be able to handle dynamic membership changes without having to reconstitute the group.

Absence of Authority - The responsibility for managing the group membership has to be devolved among members without recourse to trusted parties with delegated authority as the presence of no party can be guaranteed in any live trading context.

Robustness - Intermittent participation by members, unreliable means of communication and the absence of dependable enduring infrastructure services requires failure tolerance throughout support for system services.

Convenience - The management of group membership should not involve users in complicated and time consuming activities nor should making changes in membership status take very long periods.

7.5 Design

This section presents a fully distributed and self-organizing approach for managing group membership in ad hoc m-commerce trading systems, which is based on membership vouchers, quorate decisions by some group members, partial membership lists and the use of digital signatures.

7.5.1 Membership Voucher

A membership voucher serves as a credential that can be used by members of a particular trading forum to prove their membership to other members of the forum. It contains the following information as a minimum:-

- The trading forum name and ID.
- Its holder's trading pseudonym.
- The collection of approvals and any vetoes among verified votes. Each vote will consists of the voter's trading pseudonym, the subject of the vote either a joining request or membership renewal request, the requestor's trading pseudonym, voter's agree or disagree statement, time and date as well as the digital signature of the voter.
- Digital signature of its issuer.
- A validity period.

To be recognised as a member of a trading forum, each peer must possess a membership voucher that is digitally signed by other group members who are expected to be recognised. A recognised member is a member whose membership voucher has been verified as having the following:-

- Its validity period has not expired.
- Has been issued and signed by parties who are recognised as members at the time the membership voucher is issued.
- Has sufficient number of votes from parties who are recognised as members at the time they participated in the vote.

Peers present the voucher and their certificate to attest their membership and receiving peers use the resources available to them such as personal records of previously known members of the forum to decide whether to accept the claim. Members exchange these records with other trusted members to widen and update their views of the scope of membership. However, as the judgments are made independently by each peer based on their partial membership views without involving any authority higher than a peer, membership claims cannot always be settled to the satisfaction of all reasonable peers. It will depend on the level of trust that the receiving peers have in the issuer and the voters of the presenting peers' membership voucher as well as the parties that attest their membership vouchers. If the receiving peers trust those parties, it is expected that they will accept the presenting peer's membership claim.

The validity period of the voucher is used as a regular way to review the membership status of each member. After its expiry date has elapsed, the voucher is no longer applicable to prove a peer's membership. Thus, to remain as a current member of a particular trading forum, each peer needs periodically to renew their membership voucher when the existing voucher expires.

7.5.2 Quorate Decisions

As members of a trading forum are peers that have similar constraints on their devices and are offline most of the time, it is not realistic to expect to have a trusted peer or unbroken chain of trusted peers who are responsible for managing the group membership and are reachable all the time. All peers are given equal responsibility in order to avoid circumstances where decisions cannot be made due to the unavailability of an appropriate authority. Therefore, in this work, the decisions to accept new members, exclude misbehaving members and also renew existing

members' membership vouchers are distributed to any sufficiently large subset of existing group members. How many members need to agree and the maximum number of members allowed to disagree in order to elicit a quorate decision will depend on each trading forum's decision making policies.

A trading forum's decision making policy can be made simpler or more stringent depending on the type of ad hoc m-commerce trading. A simple policy is probably more desirable for circumstances that entail fast decision making, such as in the admission process. It may require only a small number of approval replies and no vetoes. For example, a trading forum with 30 current members may require only a small fraction of currently active and connected members to agree and none to disagree, in order to obtain a quorate decision whether to accept or reject the application of a new member. By having such a policy, new admissions could take place rapidly. On the other hand, to obtain a quorate decision for a more stringent decision making policy might require a definite higher number of approvals and less than a threshold number of vetoes. This may involve currently offline members as the replies from currently connected members may not be sufficient to obtain a quorate decision. However, to elicit the required number of members' votes may take some time as many members may not be reachable for significant periods or may not participate frequently in group communications. Thus, this type of policy might be more appropriate for circumstances that do not require rapid decision making such as in the membership renewal process or in the exclusion of members which requires more careful consideration. For example, to exclude a member from a trading forum of 40 current members might require at least 20 members to agree and less than 5 members disagree with the exclusion proposal.

7.5.3 Membership Lists

A membership list contains records about sometime members of a trading forum. It also provides information about the status of each member as to whether a member is a current member or former member or has been excluded. A complete membership list would keep members updated with the current membership of a particular group [126].

However, all members of an ad hoc m-commerce trading forum cannot be expected to have a complete and consistent view of membership as some of them may be offline or unreachable or may not participate in group communications regularly or may be active but not yet have had messages passed on to them about decisions taken by other members. Instead, members of an ad hoc m-commerce trading forum will each maintain a partial list of members and exclusions that they know about and accept in their local storage and exchange it with other members to update and

widen their view of membership every time they participate in the trading forum.

7.5.4 Digital Signature

A digital signature is used to guarantee the authenticity and integrity of a message or document sent by a peer as well as to ensure that the sender cannot get away with denying having sent the message or document. In ad hoc m-commerce trading forums, messages and documents such as membership requests, votes, membership vouchers, exclusion proposals and also exclusion orders are digitally signed by their sender in order to give assurance to the receiving peers that those messages or documents were actually sent by the specified sender and were not altered during transmission and also so that the sender will not be able to credibly deny having sent the message.

To digitally sign such documents, traders will use their private key that is self-generated during their online identity establishment process, as discussed in the Chapter 5 of this thesis. A trader's digital signature is also a part of the information in a digital certificate that binds that trader's identity credentials to his membership information.

7.5.5 Join Mechanism

For a new member to join a trading forum, he must first discover a member of the forum and then send a join request. The following steps are involved:-

Step 1. Sending a request to join

A new member (Mnew) that has appropriate ad hoc m-commerce trading software installed on his mobile device, sends a join request message together with his digital certificate to at least one member of the trading forum. Any new members that want to join the trading forum must first generate a digital certificate to establish their online identity. The certificate must be at least self-signed but may also be signed by other parties that have attested the validity of the certificate. The join request message will contain the following information as a minimum:-

- The target trading forum name and ID
- Mnew's trading pseudonym
- Digital signature of Mnew

Step 2. Propagate Join Request

Upon receiving the join request message, the contacted member (Mcontact) will verify the validity of the new member's digital certificate through trading software checks as discussed in Section 5.5.3. The contacted member may also perform the manual certificate verification check whenever it is required. After the validity of Mnew's digital certificate is verified, Mcontact will then propagate the join request message together with the verified digital certificate to other members of the forum in order to obtain a quorate decision whether to accept or reject the application. Mcontact will also include his membership voucher as a proof of his membership. The propagated message will have a time limit (TTL) in order to limit the voting period. However, Mcontact may consider having extra rounds of voting if the verified votes received are not sufficient to obtain a quorate decision after the voting period limit has expired.

In the case where the verification of Mnew's digital certificate fails, either through trading software checks or further manual checks, Mcontact is expected to discard the join request message and may multicast a warning about Mnew's attempt to gain membership with an inappropriate digital certificate together with relevant details to other members of the trading forum.

Step 3. Quorate decision by other members

Other members of the forum with views on the proposal are then expected to reply with either a signed agree or disagree message to Mcontact, accompanied by their membership voucher as a proof of their membership. This is done after they have verified the validity of both Mcontact and Mnew digital certificates as well as Mcontact's membership voucher. In addition to that, they are also expected to perform some checks on their local membership list to ensure that Mnew's identity credentials have not been used by any party that has been excluded in their membership list.

Step 4. Issuance of membership voucher

Upon receiving the replies, Mcontact will first verify that the digital signature of each voter is valid and not reported as being compromised. After the voters' digital signatures are verified, Mcontact will then verify the voters' membership vouchers as not having expired and as being of members Mcontact recognises as members or having sufficient signatures of parties Mcontact recognises as members at the time the membership vouchers were issued. Figure 7.1 depicts the steps involved in the voters' membership voucher verification process.

Votes that are not verified, or are received after the time limit, or come from a party whose digital signature is not valid or is recorded as being compromised are

discarded. Then the forum's admissions policy is applied to the verified votes. If there are sufficient acceptances and less than sufficient vetoes, Mcontact will send a signed standard membership voucher to Mnew. In addition to a membership voucher, Mcontact will also send his local partial lists of known members and known members to be excluded to Mnew.

Upon receiving the votes, Mcontact will execute the following algorithm after the validity of the digital certificate of the voters are verified;

Check whether the validity period of the voter's membership voucher is still applicable
If yes
    Check whether the voter is a recognized member in the membership list
    If yes
        Accept vote
    Else
        Check whether the voter's membership voucher is issued and signed by a recognized member at the time it is issued and has sufficient votes from recognized members at the time they participated in the vote
        If yes
            Accept vote
        Else
            Check whether the membership voucher of the unrecognized issuer and voters are issued and signed by a recognized member at the time it is issued and has sufficient votes from recognized members at the time they participated in the vote
            If yes
                Accept vote
            Else
                Discard vote
Else
    Discard Vote

Figure 7.1: Voter's membership voucher verification step

Step 5. Update membership list

Mnew will then notify other members about his new membership by multicasting a Hello message accompanied by his digital certificate and membership voucher to all currently active and connected members of the group. They will pass the multicast on during further group interactions until the multicast message's liveness expires.

7.5.6 Exclusion Mechanism

To induce participating parties in ad hoc m-commerce trading systems to act honestly and in a trustworthy way, it is valuable to have a mechanism to sanction forum members that misbehave or have a history of being given poor evaluations of their trades. One of the appropriate ways to do this is exclusion from membership. By having a mechanism to exclude misbehaving members, a group membership service can provide a degree of assurance about forum members trustworthiness and reputations. It will sit alongside the reputation system, which is one of the elements in the security and trust service for an ad hoc m-commerce trading system, and serves as the primary service to help assess the behavior and also the trustworthiness of each member. Similar to the join process, to exclude an existing member requires a quorate decision from other members of the trading forum. The following steps are involved:-

Step 1. Multicasting a proposal to exclude

An existing member (Mpropose) can propose to exclude a misbehaving member or a member with poor evaluations from a trading forum by multicasting a proposal to exclude message to other forum members including the target member (Mtarget). The message will consist of the following information:-

- The target member's trading pseudonym.
- Mpropose digital signature

In addition to that, an accompanying note giving brief reasons and some relevant evidence for the exclusion might also be expected.

Step 2. Quorate decision by other members

If other forum members agree or disagree with the exclusion proposal, they will reply with a signed agree or disagree message (vote) to Mpropose within the required time period. Each vote will consists of the voter's trading pseudonym, the subject of the vote which is exclusion proposal, the requestor's trading pseudonym, voter's agree or disagree statement, time and date as well as the digital signature of the voter. In addition to that, the trading pseudonym of the target party to be excluded will also be included in the message. The target party can take this opportunity to rebut the proposal by sending a disagree vote to Mpropose and also multicast a message and supporting evidence to other members in order to defend himself from being excluded from the trading forum's membership.

Step 3. Multicasting an exclusion order

Once enough replies from validated members are collected within the voting time period limit and the forum's exclusion criteria are satisfied, Mpropose will then multicast an exclusion order to other currently connected members with the intention that they forward it more widely to other members when they next connect to the forum. The exclusion order will have the following details:-

- The target party's trading pseudonym
- The collection of signed messages approving and disapproving the target's exclusion
- The reason of the exclusion
- Digital signature of Mpropose
- Exclusion period

Mpropose is also expected to attach the target party's digital certificate together with the exclusion order so that other parties who do not have any record about the target party's identity credential in their local repository can use it for future reference. In this case, forum members are expected to refrain from issuing a new membership voucher to the target member after the validity period of his current membership voucher has expired until the exclusion period has ended. Also, any votes or membership vouchers issued by the target member will not be considered as valid. Furthermore, forum members are also expected to not participate in any transactions with that member.

7.5.7 Membership Renewal Mechanism

To remain as a member of a trading forum, each member should renew their membership near the end or after the validity period of their current membership voucher expires. The following steps are involved:-

1. Sending a membership renewal request

A member who holds an expired or soon to expire membership voucher sends a membership renewal request together with his old or current membership voucher to at least one of the current members of the trading forum (Mcontact).

2. Propagate Renewal Request

Similar to the join and exclusion mechanisms, to renew a membership voucher also requires a quorate decision from other forum members. Thus, upon receiving the

membership renewal request, Mcontact will then propagate it to other forum members in order to obtain a quorate decision whether to accept or reject the renewal request.

3. Quorate decision by other members

In this situation, other members are expected to check whether any non-expired order has been issued to exclude the requesting member from the trading forum before they each reply with either a digitally signed agree or disagree message together with their valid membership voucher to Mcontact.

4. Collate agree messages

Once enough replies from validated members are collected within the voting period limit and the forum's membership renewal criteria are satisfied, Mcontact then collates the replies and sends them together with a new membership voucher to the requesting member. The voucher is signed by Mcontact as an accurate record of the vote. The requesting member is then expected to multicast his new membership voucher to other members of the trading forum to inform them about the renewal of his membership.

7.5.8 Message Propagation

In this work, each message is associated with a unique identifier and a time to live (TTL). To ensure reliable message propagation, each time a peer receives a message for the first time, it will accept the message, store it and also forward it once to each of its directly connected neighbours except the sender during the period of its lifetime. To prevent duplicate propagation, each time a peer receives the same message more than once, the message will be discarded. As all of the mechanisms discussed above require sufficient members votes to obtain a quorate decision, it is important for each voting activity to have an expiry time. Therefore, the use of a TTL will ensure that each propagated message is discarded after its time limit has expired.

7.6 Reference Scenarios

This section demonstrates each of the mechanisms discussed in Section 7.5 in a series of scenarios; namely joining scenario, exclusion scenario and renewal scenario.

7.6.1 Joining Scenario

A trading forum A consists of 5 members M1, M2, M3, M4 and M5. All members are online during communication period t1. It is assumed that:-

- Each of them possesses a valid digital certificate and current membership voucher.
- Each of them has appropriate ad hoc m-commerce trading software installed on their Wi-Fi enabled mobile device.
- Each member's local membership list contains the membership records of other members as follows:

  M1 (M2, M3, M4, M5)

  M2 (M1, M3, M4, M5)

  M3 (M1, M2, M4, M5)

  M4 (M1, M2, M3, M5)

  M5 (M1, M2, M3, M4)
- No member has any knowledge of parties to be excluded.
- This trading forum applies a simple admissions policy that requires at least three members agree with the new application and none disagrees while votes are being gathered.

A new member M6 comes into their communication range and sends a join request to M2 together with his self-signed digital certificate. After verifying and attesting M6's self-signed digital certificate, M2 then propagates the request to other members, as illustrated in Figure 7.2.

It is assumed that all members agree to accept the new application from M6 after verifying its digital certificate and M2's digital certificate and membership voucher. They then each reply to M2 with their digitally signed agree message together with their membership voucher. Upon receiving the replies, M2 will then verify each of the voters' digital certificates and membership vouchers. In this case, all votes are accepted as each of the voters possesses a valid digital certificate and current membership voucher and M2 recognises them all as members in his membership lists. M2 then applies the trading forum's admissions policy to the verified votes and sends a signed standard membership voucher containing the four signed approvals and its local membership list to M6. These steps are illustrated in Figure 7.3.

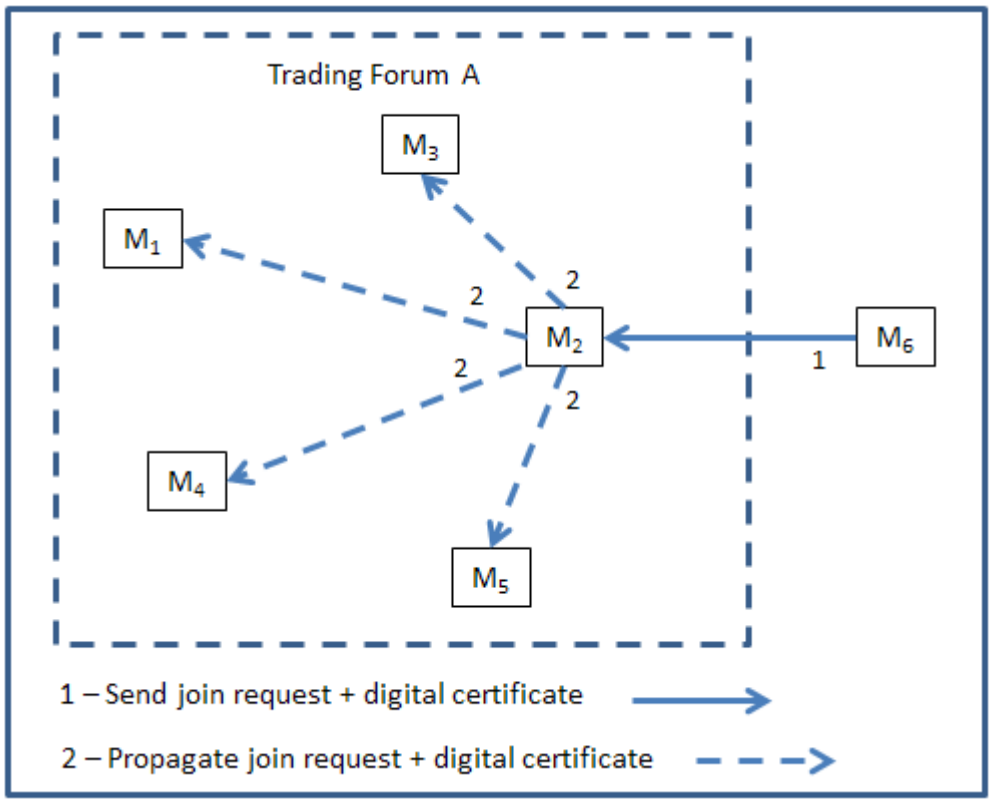


Figure 7.2: Join mechanism - steps 1 and 2

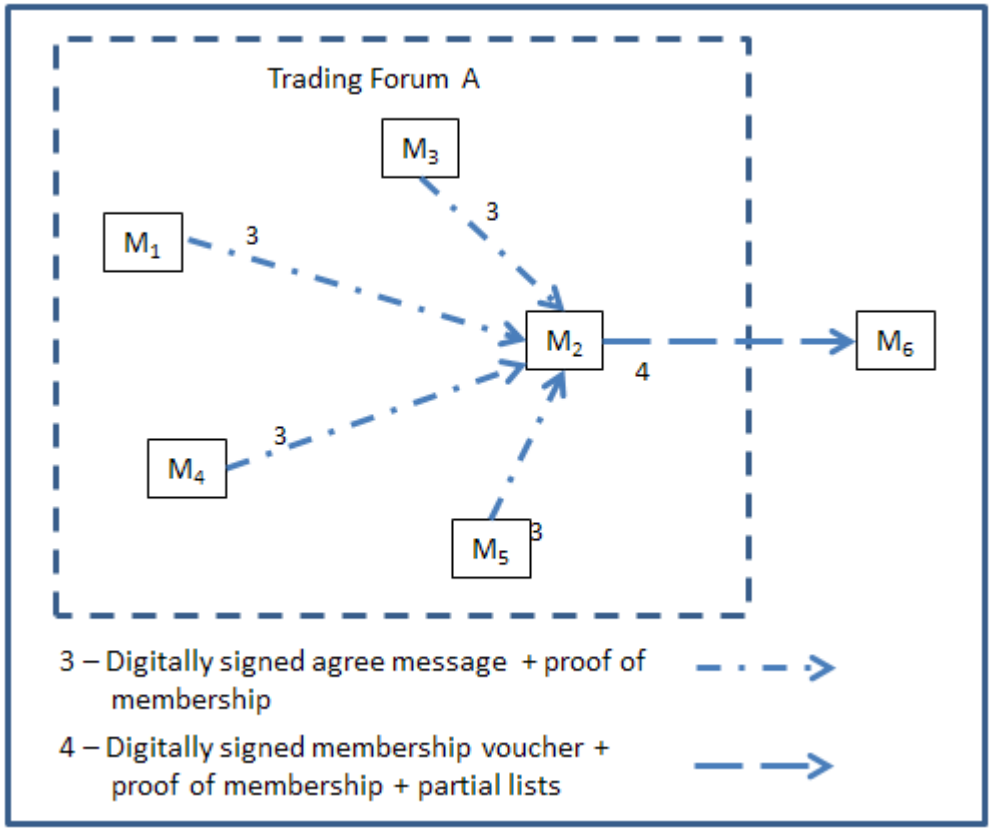


Figure 7.3: Join mechanism - steps 3 and 4

M6 then sends a hello message together with his digital certificate and membership voucher to other connected members in order to notify them of his new membership, as illustrated in Figure 7.4. Upon receiving M6's hello message, digital certificate and membership voucher, other connected members will independently verify M6's digital certificate and membership voucher before accepting the new membership and update their local membership list. At the end of communication period t1, the local membership list of each member will be as follows:-

M1 (M2, M3, M4, M5, M6)

M2 (M1, M3, M4, M5, M6)

M3 (M1, M2, M4, M5, M6)

M4 (M1, M2, M3, M5, M6)

M5 (M1, M2, M3, M4, M6)

M6 (M1, M2, M3, M4, M5)

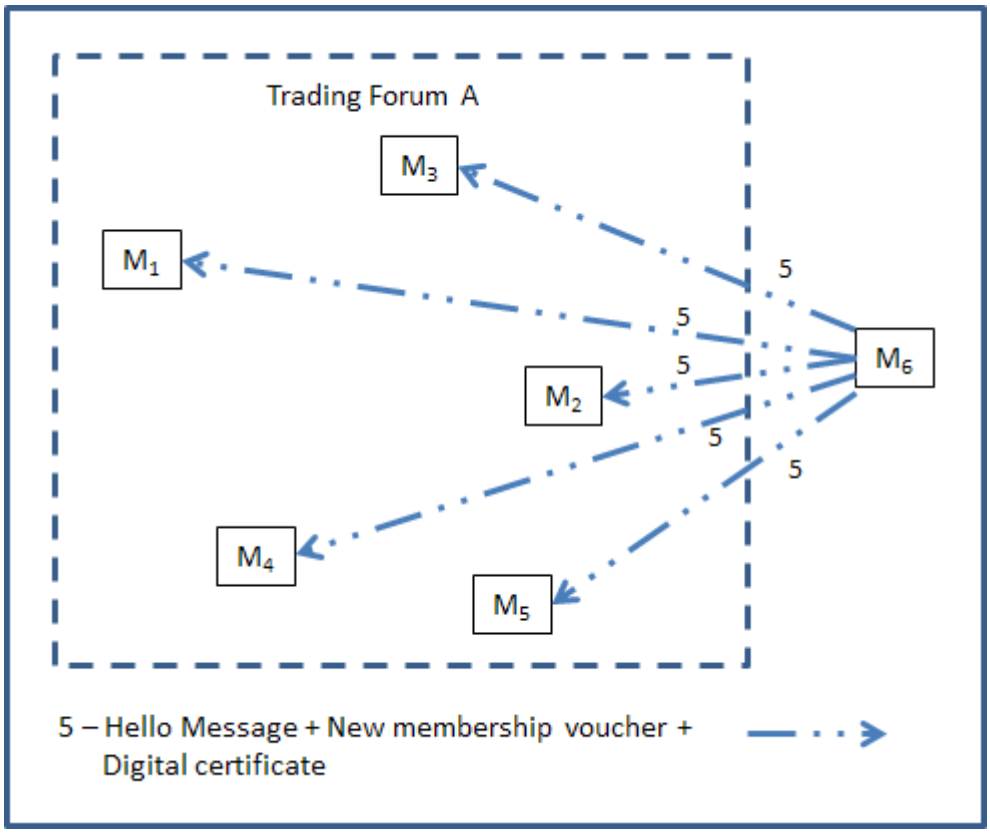


Figure 7.4: Join mechanism - step 5

7.6.2 Exclusion Scenario

This scenario takes place after the earlier one. It is assumed that:

- During this communication period, trading forum A consists of 20 parties (M1, M2, ..., M19 and M20) that possess a current membership voucher. However, only ten members M1, M2, M3, M4, M8, M10, M15, M16, M17 and M19 are online while the others have gone offline.
- This trading forum applies an exclusion policy that requires at least 7 members to agree with the exclusion and less than 3 vetoes before any member can be excluded.
- The local membership list of each currently connected member contains the membership record of other connected members as each of them needs to send a hello message together with their membership voucher to all connected members in order to rejoin the trading forum after being offline or disconnected from the network.

M2 multicasts a proposal to exclude M8 together with relevant evidence to all currently connected members of the forum. It is assumed that all reply except M16 after the validity of M2's certificate is verified and only M1, M3, M4, M10, M15 and M19 agree with the exclusion proposal while the other two members including M8 disagree, and M2 receives their digitally signed votes within the voting period limit. Upon receiving the votes, M2 then verifies the voters' digital signatures and membership voucher. M2 then accepts their votes as their digital signatures are valid and not recorded as being compromised, the validity period on their membership vouchers are still applicable and M2 recognises them all as members in his local membership list. After adding his own approval vote and the forum's exclusion policy is applied, there are sufficient number of approvals (7 approvals) and less than sufficient vetoes (2 vetoes) for M2 to obtain a quorate decision to issue an exclusion order. M2 then multicasts the exclusion order together with M8's digital certificate to all connected members. This scenario is illustrated in Figure 7.5, Figure 7.6 and Figure 7.7.

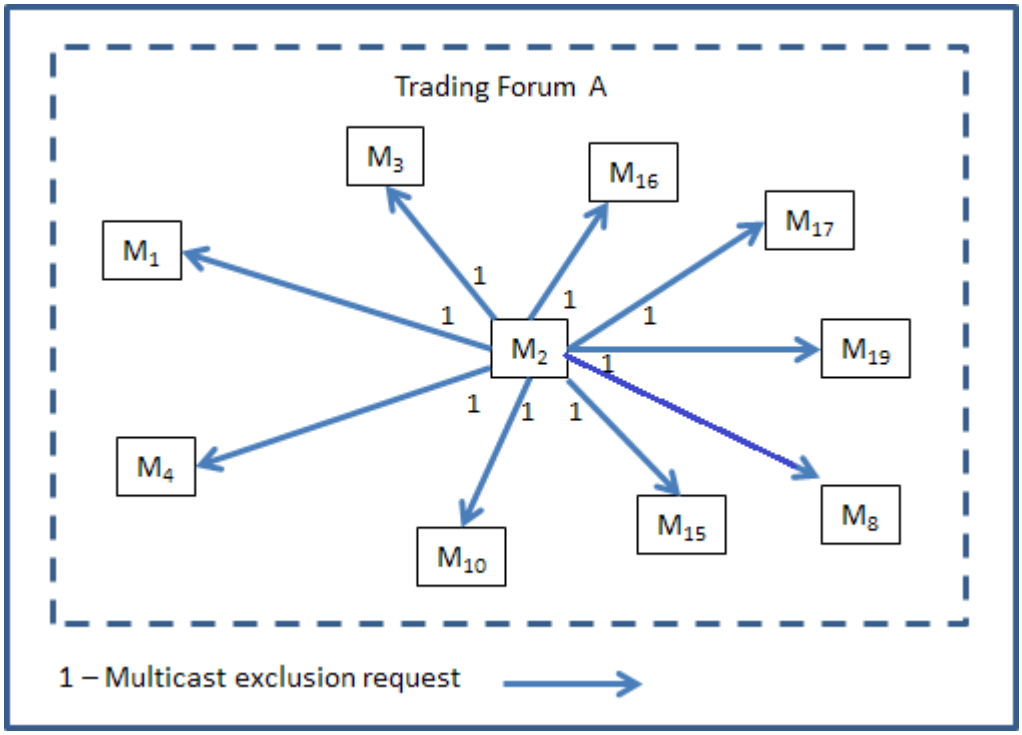


Figure 7.5: Exclusion mechanism - step 1

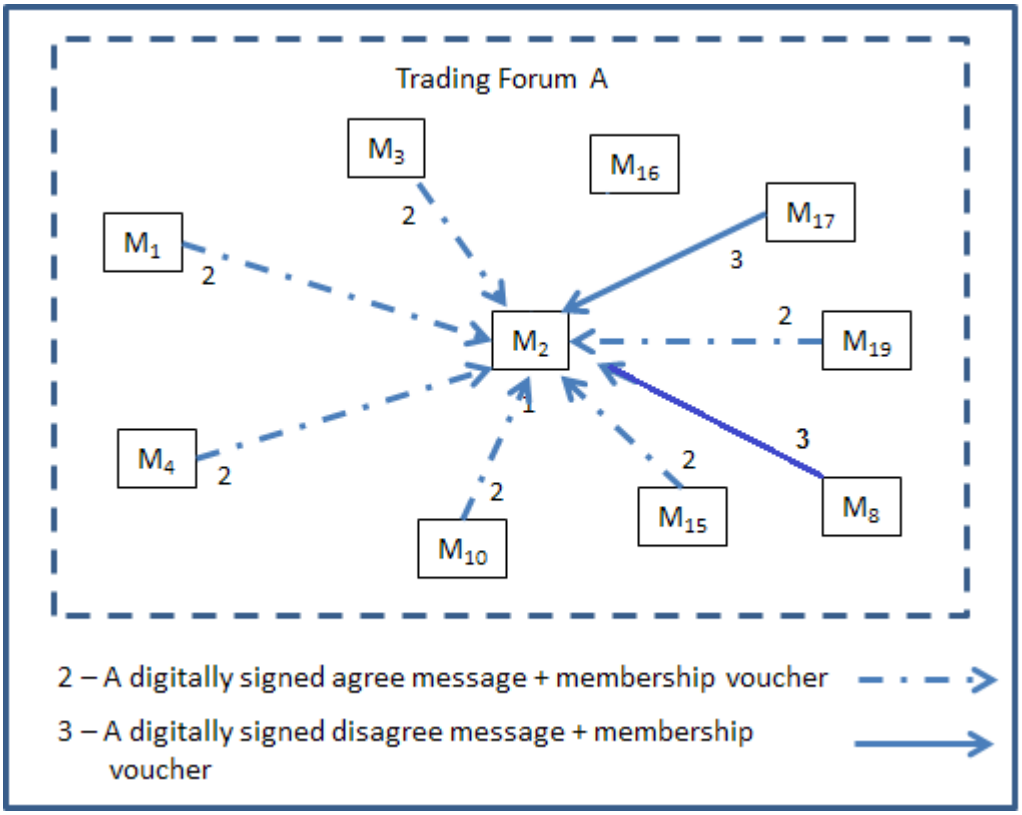


Figure 7.6: Exclusion mechanism - step 2

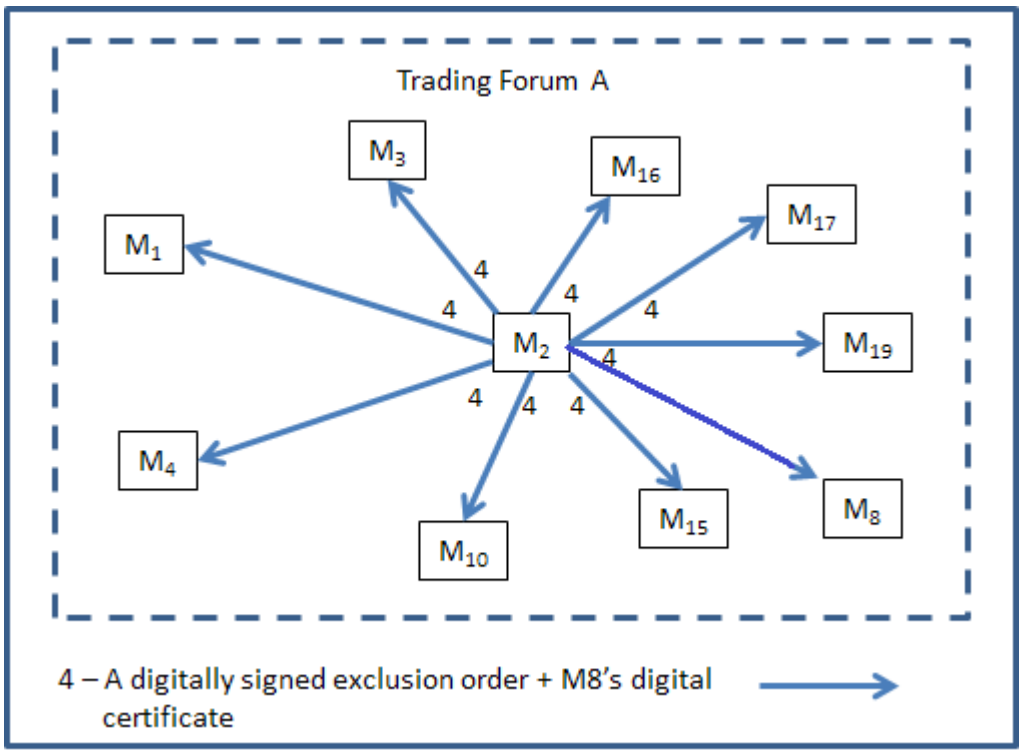


Figure 7.7: Exclusion mechanism - step 3

7.6.3 Renewal Scenario

In this scenario, trading forum A consists of 25 current members (M1, M2, ...M7, M9, ... , M25) and it is assumed that:

- In the beginning, only M1, M4, M6, M7, M9 and M10 are online while the others are offline.
- M1's membership voucher is nearly expired.
- Renewal policy requires at least 7 members to agree with the renewal request and no vetoes before any new membership voucher can be issued to the requesting member.

M1 sends a membership renewal request together with his current membership voucher to M9 who then propagates the request to other currently connected members. It is assumed that only M4, M6 and M7 agree with the request and reply with a digitally signed agree message together with their membership voucher to M9 as depicted in Figure 7.8. It is assumed that M10 received the propagated message but decided not to participate in the vote. Upon receiving the agree replies, M9 then verifies M4, M6 and M7s membership vouchers and accepts their votes as the validity period on their membership voucher is still applicable and M9 recognises them

as members in his local membership list. However, in this situation, the number of approval replies is still not sufficient for M9 to obtain a quorate decision to issue a new membership voucher to M1. Thus, M9 has to wait until the voting period limit expires before he can consider a second round of voting.

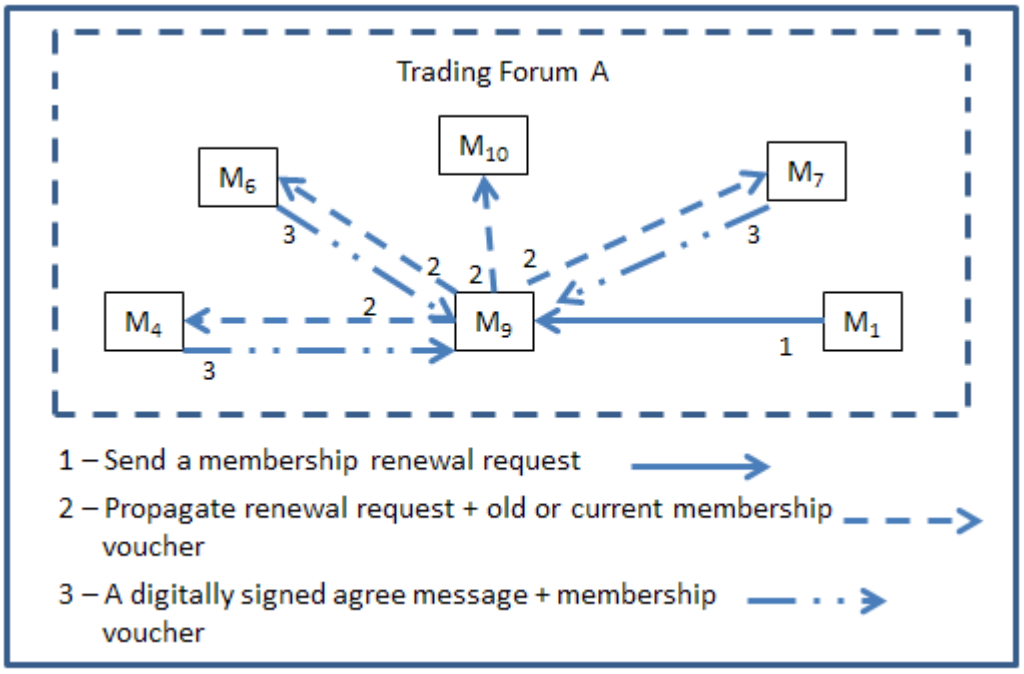


Figure 7.8: Renewal mechanism - steps 1, 2 and 3

After some further time has elapsed within the same voting period limit, it is assumed that M4, M6, M7 and M10 have gone offline while M2, M5, M20, M23, and M25 come into communication range with M1 and M9. The others remain offline. M9 then propagates the membership renewal request to M2, M5, M20, and M23 after receiving their Hello Message and verifies their membership voucher. In this case, it is assumed that M9 did not accept M25's membership claim as he did not recognise either the issuer of M25's membership voucher or the issuer and voters of that issuer as members in his membership list. Thus, the renewal request is not propagated to M25. M2, M5, M20, and M23 agree with the request and they each reply with a digitally signed agree message together with their membership voucher to M9 within the voting period limit. M9 then validates their votes. Validated votes from M2, M5, M20, and M23 as shown in Figure 7.9 now enable M9 to obtain a quorate decision to issue a new membership voucher to M1.

7.7 Security Analysis

The aim of having a group membership service for ad hoc m-commerce trading systems is to improve the security of such trading systems by restricting participation

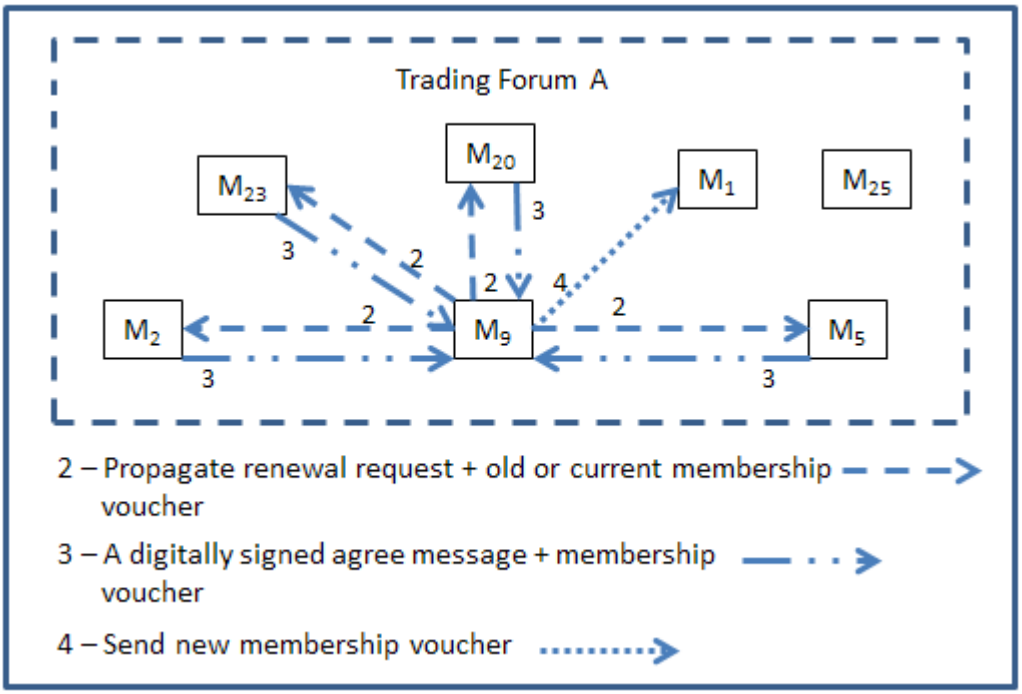


Figure 7.9: Renewal mechanism - steps 2, 3 and 4

to only parties that are regarded as trustworthy by their peers. However, as there is no network service provider that can be relied upon to provide such service and the task for managing it has to be devolved among participating parties of the trading system, it is crucial that no one can compromise the reliability of such a membership service.

Thus, this section examines the means by which the ill-intentioned parties in an ad hoc m-commerce trading system can pose threats to compromise the reliability of its membership service and discusses how the proposed design of a membership service and also identity support scheme can detect and mitigate such threats to a sufficient degree.

7.7.1 Addressing Whitewashing

The objective to constrain the trading system's participation to only traders that trust each other might not be successful if a trader that has been excluded from a trading forum membership due to his poor reputation or misbehaviour can easily re-join the trading forum using a new identity. There are at least two ways that such ill-intentioned trader can re-join the trading forum using the proposed approach:

7.7.1.1 By Working Alone

In this situation, an ill-intentioned trader will send a join request message together with his new self-signed digital certificate to any of the trading forum members that are online and within his communication range. The contact person who receives the join request message is then expected to verify the validity of the self-signed digital certificate through a certificate attestation process as discussed in Section 5.5.3.1, before propagating it together with the join request message to other members. The trading software checks in the attestation process should enable the contact person to detect whether this is an attempt by the presenting party to re-enter the trading forum with a new identity. This will alert the contact person to perform further checks with his membership list to verify whether the identity credentials in the presented certificate, especially the photograph has been used by other party that is recorded as being excluded in his membership list. A physical meeting with the presenting party will give further verification about the similarity of the photograph of the excluded party with the physical appearance of the presenting party.

However, the contact person might not be able to detect such an attempt if he does not have any record about the ill-intentioned party's digital certificate and/or membership information in his local repository due to the following reasons:

- They have never encountered each other or had a deal before.
- The contact person does not have a copy of the presenting party's certificate in his local certificate repository, or has not yet been passed the updated membership list or the exclusion order for the ill-intentioned party from other members of the trading forum.

In this case, the contact person is expected to propagate the join request message without attesting the ill-intentioned party's self-signed digital certificate. This will alert the other parties who are participating in the vote to verify the validity of the self-signed digital certificate properly before accepting the join request. Again, the trading software and further manual checks in the attestation process, as well as the membership list checks should enable the traders to detect such an attempt and help them to make a decision to reject the join request application. Thus, it will be less likely for the contact person to obtain sufficient votes to issue a membership voucher to the ill-intentioned party.

7.7.1.2 By Colluding with Associates

Another way for a member that has been excluded from a trading forum's membership to re-join the trading forum is by choosing his associate to be the contact person to propagate his join request message to other members of the trading forum. In this case, as they are associates, the contact person is likely to just ignore any alerts given by the trading software checks regarding the identity credentials in the ill-intentioned trader's self-signed digital certificate before propagating the join request message to other members. The contact person might also attest the self-signed digital certificate to support that the validity of such certificate has been verified and the join request message does not come from a suspicious identity.

However, the other members who view the join request message should be able to detect such an attempt when they perform the trading software checks and also further checks in the authentication process of the digital certificate, as discussed in Section 5.5.3.2. Checks with their local membership list will further verify that the identity credentials in the presented digital certificate have been used by another party that is recorded as being excluded in their membership list. This can be used as an evidence that the contact person is colluding with the excluded member to compromise the membership service and thus, the contact person is also risking being subject to being excluded from the trading forum's membership due to his misbehaviour.

In addition to the above, it is also possible for the ill-intentioned trader to collude with a number of associates to enable him to re-join the trading forum. In this case, one of the associates will be the contact person and the others will participate in the vote. If the votes from their associates are sufficient to enable the contact person to obtain a quorate decision to accept the join request, the ill-intentioned party will be able to get a new membership voucher to enable him to re-join the trading forum. However, the other members of the trading forum who receive the new membership voucher may well be able to detect such an attempt when they verify the validity of the ill-intentioned party's digital certificate and also perform some checks with their local membership list. Again, this can be used as an evidence that the signer of the new membership voucher and its voters are colluding with the ill-intentioned party to manipulate the group membership decision making process and thus, they are risking being subject to being excluded from the trading forum's membership due to their misbehaviour.

7.7.2 Addressing Unfair Exclusion

There are at least three ways that an ill-intentioned trader can attempt to use to unfairly exclude a particular trader, for example an honest trader from the trading forum's membership, which include the following:

7.7.2.1 By Using his Own Identity

An ill-intentioned trader uses his own identity to multicast a proposal to unfairly exclude another trader from a trading forum's membership. In this case, it will be a bit difficult for other members of the trading forum to detect such an attempt if the ill-intentioned trader has the following elements;

- A valid digital certificate and membership voucher.
- A good reputation established by a series of favourable deal evaluations.
- Never received any complaints of misbehaviour from other members of the trading forum.
- Never been the subject of an exclusion proposal

However, as the proposed approach advises that relevant evidence to support an exclusion proposal be sent together with it, it is less likely that the ill-intentioned trader will be able to obtain sufficient votes for the exclusion from other members of the trading forum if he fails to provide such important evidence. In addition to that, it is a bit risky for the ill-intentioned trader to use his own digital signature to sign such a proposal. This is because his digital signature on the proposal will ensure that he is accountable for what he has done and if the other traders find out that the proposal is used to unfairly exclude another trader, they can use it as an evidence to exclude him in turn from a trading forum's membership for his misbehavior.

7.7.2.2 By Using a Spoofed Identity

An ill-intentioned trader uses another trader's identity, for example, the identity of a respectable trader to multicast an unfair exclusion proposal to other members of the trading forum. He can do this if he gets hold of the respectable trader's private key. In this case, when the other traders who receive the proposal perform some checks on the credibility of its sender, it is unlikely that they will be suspicious of the proposal as it comes from a credible and reputable trader in the community.

However, they might just ignore the proposal if no relevant evidence is sent together to support the proposal. In addition to that, the trading software checks in the authentication process of the sender's digital certificate may enable them to detect that his digital certificate is recorded as suspected compromised in their local repository. If they perform further checks by physically meeting with the sender, they will be able to identify the real identity of the sender based on his physical appearance. Again, this can be used as an evidence to exclude the ill-intentioned party in turn from the membership of the trading forum for his misbehaviour.

7.7.2.3 By Colluding with Associates

Another tactic that an ill-intentioned trader can use to try to unfairly exclude another trader from a trading forum's membership is by colluding with his associates in the voting process for the exclusion. In this case, the ill-intentioned trader or one of his associates will multicast the unfair exclusion proposal and the other associates will participate in the vote in order to manipulate the decision making process. While the other members of the trading forum who are also participating in the vote might just ignore the proposal if it is not supported with relevant evidence, the associates will reply with their agree message in order to obtain a quorate decision for such an unfair exclusion attempt to be successful. This possibility remains challenging to address as it involves a conspiracy among a group of accomplices that can influence the group decision making process.

However, a stringent exclusion policy that requires a large number of agree votes will help diminish the possibility of such unfair exclusions. This is because the ill-intentioned traders would require significant numbers of associates in order to obtain a quorate decision for the exclusion.

7.7.3 Addressing Integrity Issue of a Vote

The integrity of each trader's votes is another important issue that needs to be addressed to ensure the reliability of the proposed group membership service, as it may influence the group decision making process to obtain a quorate decision. There are at least two possible ways that the integrity of a vote can be compromised, which include the following:

7.7.3.1 Altered By a Contact Person

A trader that acts as a contact person might change the content of the votes that he received from other members of the trading forum in order to manipulate the group membership decision making process, for example in the voting process of a membership renewal. By changing the content of some or all of the votes from disagree to agree, the contact person would be able to obtain sufficient votes to issue a new membership voucher to his associate although the majority of the voters have actually given their disapproval for such renewal request.

However, as each vote is digitally signed by its sender, the contact person needs to steal or compromise the voters' private keys in order to correspondingly change the signatures on the contents of the votes that he received, which is not an easy thing to do. To accomplish the task requires some knowledge and technical skills with cryptographic keys, as well as an appropriate tool or program.

In addition to that, the other traders who receive the new membership voucher may be able to detect that the private key used to digitally sign some or all of the votes has been reported to be compromised when they check the validity of the digital certificates of the new membership voucher's signer and voters. The trading software checks in the authentication process of the digital certificates will alert the traders that the private key for those certificates have been recorded as being compromised in their local certificate repository.

7.7.3.2 Altered By an Intermediary Peer

An ill-intentioned trader that acts as an intermediary peer might try to change the content of the votes that are transmitted through his node in order to subvert the reliability of the group membership decision making process. However, as traders are expected to encrypt each of their votes with the public key of the recipient before sending them to the recipients, it will be a challenging task for the intermediary peer to alter the content of such encrypted votes. Furthermore, the digital signature of the sender that is used to digitally sign the votes will ensure that any alteration made to the votes during transmission will be detected by the recipients. This check will require the recipient to have a digital certificate for the sender.

7.8 Discussion

This section discusses the things that a trader in an ad hoc m-commerce trading system should do to mitigate some of the threats that can subvert the reliability of its group membership service.

7.8.1 Essential Recommendations When Dealing with Membership Vouchers

Before accepting any membership claim from any traders, traders of an ad hoc m-commerce trading system are expected to do the following:

1) Verify the validity of the digital certificate of the presented membership voucher's holder to ensure that there is no attempt from any parties to re-join the trading forum after being excluded from membership.

2) Verify the validity of the digital certificates of the presented membership voucher's signer and also its voters to ensure that only parties that have a valid identity participated in the decision making process to issue the membership voucher.

3) Verify the membership status of the presented membership voucher's signer and also its voters to ensure that it is issued by a recognised member and has sufficient number of votes from recognised members at the time they participated in the vote.

4) Discard any membership voucher that fails to satisfy any of the above verification processes.

7.8.2 Essential Recommendations When Participating in Group Membership Decision Making Process

Traders of an ad hoc m-commerce trading system are expected to do the following when they are involved in any of the voting processes for group membership;

7.8.2.1 As a Contact Person

A trader that acts as a contact person for either a join request or membership renewal request, is expected to do the following before propagating the request message to the other members of the trading forum.

1) Verify the validity of the digital certificate of the party who sends the request

message, especially the join request message to ensure that there is no attempt by the sender to re-join the trading forum after being excluded from membership.

2) Do not attest any self-signed digital certificate from a self-professed new member if unsure about the identity credentials in the certificate. This is to avoid the possibility of being involved in an attempt by an excluded member to re-join the trading forum after being excluded from membership.

3) Check the local membership list to ensure that the requestor is not in the list of parties that are recorded as being excluded or as being subject to a valid exclusion proposal.

7.8.2.2 As a Voter

Traders that are participating in the group decision making process are expected to do the following before giving their digitally signed approval or disapproval for any requests or proposals;

1) Verify the validity of the digital certificate of the party who sends the request message, especially the join request message to ensure that there is no attempt by the sender to re-join the trading forum after being excluded from membership.

2) Verify the validity of the digital certificate of the party who acts as a contact person, especially in the exclusion proposal to ensure that there is no attempt by that party to spoof another trader's identity to avoid from being accountable for any unfair exclusions.

3) Check the local membership list to ensure that both the requestor and contact person are not in the list of parties that are recorded as being excluded or a subject in the exclusion proposal.

7.9 Conclusion

This chapter discusses the values of constraining an ad hoc m-commerce trading system participation by using a group membership service in order to establish greater trust and more secure interactions among its group members. It also proposes a design for a group membership service that does not rely on a complete knowledge of the current group membership to determine whether a peer is a member of a particular trading forum. The proposed approach does not demand all group members participate in group communications frequently and regularly in order to obtain a quorate decision for managing group membership.

However, as the attestation process does not involve any authority higher than a peer and is done independently by each peer based on their partial knowledge of group membership, membership claims acceptable to a sufficient number of peers to qualify may not be found acceptable by all other reasonable peers.

This chapter has reviewed the means by which ill-intentioned parties can threaten to compromise the reliability of the group membership service. It has shown that appropriate checks can exclude nearly all threats except for those involving very extensive collusion among enough parties to meet the trading forum's membership support requirements. With support from the proposed identity support scheme [119] and reputation system, the aim is to propose that this type of group membership service could be effectively used to improve the security of ad hoc m-commerce trading systems by restricting participation to parties regarded as trustworthy by their peers.

Chapter 8

Sharing Knowledge About Potential Threats in an Ad Hoc M-Commerce Trading Community

8.1 Introduction

In an ad hoc m-commerce trading system, although its security services such as the identity support scheme, reputation system and group membership service can ensure the security of the trading system to a sufficient degree for traders to participate in its transactions, it cannot be assumed that all traders will always behave properly and conform to the trading system's rules and regulations. There might be some traders who misbehave or breach the norms of acceptable trading behaviour, which could subsequently pose potential threats that would undermine the functionality and reliability of such security services. As there is no party who is specially trusted that can be relied upon to monitor each of the trader's behaviour in such a loose ad hoc trading community, having a mechanism that allows traders to share their knowledge about suspected misbehaviour or malpractice would help to mitigate or avoid any undesirable consequences or potential threats due to a trader's misbehaviour or malpractice. One way to accomplish this is through the use of security warnings or alerts.

Warnings or alert messages can be used to inform traders about potential threats or risks in their transactions, so that they can take the necessary actions to mitigate or avoid such threats or risks. Such messages can also serve as a reminder to influence traders to behave properly and act honestly in each of their transactions and activities in the trading system, which will subsequently improve the security of the trading system. This is because if they are detected or suspected to have mis-

behaved, the information about their misbehaviour might be shared among other traders and they might lose their reputation or opportunities to trade or be excluded from the trading system. Thus, in order for them to maintain their good reputation and so on, they need to behave properly and conform to the trading system's rules and regulations.

However, the use of security warnings or alerts in such a loose ad hoc m-commerce trading community may raise some issues. This is because traders may broadcast warnings or alert messages based on their suspicions that are not well founded, which could then raise the issues of libel as there could be an innocent explanation from the accused parties for the actions that they have done. In addition to that, ill-intentioned traders may misuse the warnings or alert messages to bully other traders or to unfairly blacken their reputation, which could subsequently cause a lot of conflicts as the accused parties may attempt to rebut such accusations. The accused parties are likely to generate lots of responses to defend themselves from the accusations and this may cause the network traffic to be heavy with such messages.

Thus, in order to mitigate the above-mentioned issues, the security warning scheme for an ad hoc m-commerce trading system needs to frame a warning or an alert message in a way that lets it perform its intended function without raising further problems. The message also needs to be expressed in a reasonably neutral language and an easy to understand format, and supported with sufficient evidence in order for it to be considered by the receiving parties. In addition to that, the accused parties should be given an opportunity to respond to the accusation by giving their short signed explanation in the message.

The remainder of this chapter is structured as follows. Section 8.2 presents the security warning scheme for an ad hoc m-commerce trading system. Several reference scenarios are discussed in Section 8.3. Section 8.4 discusses the things that a trader should and should not do when dealing with warning or alert messages and finally, Section 8.5 concludes this chapter.

8.2 A Security Warning Scheme for an Ad Hoc M-Commerce Trading System

This section discusses a detailed scheme of reporting, disseminating and acting on warnings about suspicious behaviour of a trader or suspected lapses of security. Any trader detecting such misbehaviour and have sufficient supporting evidence or uncontestable facts about it may choose to notify other traders in the trading system about the potential threats by multicasting an alert message. This will allow

the traders who are exposed to the threats to be aware of their risks and take the necessary actions to avoid or mitigate those risks.

Traders can generate an alert message by instantiating it from a standard form approved by the trading forum. A standard form of an alert message should contain at least the following types of information:

- The trading forum's name.
- The communication scope to disseminate the alert message.
- The author's trading pseudonym and date joined the trading forum.
- The date and time the alert message is generated.
- The subject or title of the alert message such as failure of a check in attesting a certificate, failure of a check in verifying a membership voucher and so on.
- The target party's trading pseudonym and date joined the trading forum.
- The type of the failures detected such as public key and self-signed signature mismatch, photo in a presented certificate matches with a photo of another identity in the local certificate repository, the content of a membership vote is suspected to have been altered etc.
- The potential impact or consequences of the failures to a trader or the trading community, in terms of loss of reputation or customers, or its influence to the certificate attestation or authentication processes, membership group decision making processes, and so on.
- The date and location the incident takes place.
- Short description on the incident and how the failure was detected.
- Short comments on the incident.
- Recommended actions to be taken by the recipients, such as to save the suspicious certificate in the list of certificates that have been broadcast alerts about, to exercise caution before relying on a membership voucher etc.
- Attached documents as evidence to support the alert message. Warning or alert messages without any supporting evidence should not be considered.
- Short signed explanation or comments by the target party. Alerts without signed repostes in them should be judged as less satisfactory because the target party has not added any response.

- The digital signature of the author to ensure that he cannot credibly deny having sent the warning message.

Trading Group:	Easy e-Flea Market
Communication Scope:	Multicast to all members
From:	Sneaky Pete — Member since: January 01, 2013
Date Sent:	Saturday, August 24 2013 11:00 am
Subject:	Failure of a check in attesting a certificate.
Type of Failure:	Photograph in a certificate is found to be matched with a photo of another identity.
Concerning:	The Professor — Member since: N/A
Harm Done:	None
Occasion, Date and Place:	Certificate Attestation Request, Friday, August 23, 2013 at Grill House Café, Paris
Description:	A new certificate (Cert10) presented by a trader, the Professor is found to have a similar photo appearance with a photo in another identity's certificate (Cert03 - Brainy Barnes) that has been issued an exclusion proposal, when trying to get the new certificate attested. Physical appearance of the presenting party is similar to the photo in the presented certificate.
Comment:	It seems that the presenting party and the owner of the existing certificate in my local certificate repository are the same person.
Recommended Actions:	Save Cert10 in the list of certificates that have been broadcast alerts for future reference.
Attached Documents / Evidence:	Cert10, Cert03.
Comment by: The Professor	The private key of my old certificate has been compromised. I was trying to revoke my old certificate but mistakenly sent it as a new certificate for a new identity. Digital Signature: The Professor
Author's Digital Signature:	Sneaky Pete

Figure 8.1: A warning or alert message example

Figures 8.1 and 8.2 illustrate two examples of an alert message that might be sent due to a failure in a certificate attestation check. The parties who receive the message are then expected to perform the following:

1) Verify the identity of the author of the warning or alert message through a certificate authentication process as discussed in Section 5.5.3.2, before deciding to store or discard or forward it to other traders. If all the checks in the authentication process are satisfactory, the sender is a credible party and there is sufficient evidence

Trading Group:	Easy e-Flea Market
Communication Scope:	Multicast to all members
From:	Sneaky Pete Member since: January 01, 2013
Date Sent:	Saturday, August 17, 2013 11:00 am
Subject:	Failure of a check in attesting a certificate.
Type of Failure:	Public key and self signature of a certificate don't match.
Concerning	Honest Jones Member since: N/A
Harm Done:	None
Occasion, Date and Place:	Certificate Attestation Request, Friday, August 16, 2013 at Grill House Café, Paris
Description:	The self signature on a digital certificate presented by a new trader, Honest Jones (cert01) is found to be mismatched with its corresponding pubic key during the certificate attestation process.
Comment:	Honest Jones did not apologise.
Recommended Actions:	Save cert01 in the list of certificates that have been broadcast alerts about and mark it as "suspected compromised" for future reference.
Attached Documents / Evidence:	cert01
Comment by: Honest Jones	It was an honest mistake. I signed it with the wrong key because I got confused. Digital Signature: Honest Jones
Author's Digital Signature:	Sneaky Pete

Figure 8.2: Another example of a warning or alert message

to support the message, the recipients are expected to store the warning or alert message for future reference and forward it to other traders. Otherwise, they may choose to ignore or discard the message.

2) Forward the message to other traders at later junctions until the message's liveness expires to ensure that those who missed the alert message have another chance to receive it, or those who ignored an earlier message, have another opportunity to reconsider it.

8.3 Reference Scenarios

8.3.1 Failure in a Certificate Attestation Check

Consider the scenario where the trading software check in step 4 in Section 5.5.3.1 (A) finds that a photo in a presented certificate is similar to the photo of an existing identity in the local certificate repository and further checks done by the attestor on the existing identity's certificate finds that it has been issued with an exclusion proposal. Furthermore, when the attestor meets with the presenting party in person, it is found that his physical appearance is similar with the photo in both certificates. In this case, it could be an attempt by the presenting party to re-enter the trading forum with a new identity and thus, the attestor should refuse to sign the presented certificate. However, the presenting party may then request another trader to attest his new certificate and if that trader does not have the certificate of the other identity in his local certificate repository, he may sign the presented certificate.

In such a case, if the first attestor multicast a warning or an alert message as illustrated in Figure 8.1 to other traders in the trading forum, it could alert them to be careful and take the necessary actions if they receive a certificate attestation request from the same party. If there is an attempt by the presenting party to re-enter the trading forum with a new identity, this could reduce the likelihood of such an attempt to be successful. The short signed explanation or response by the target party will help the relying parties to consider whether the issue being expressed in the message is satisfactory or not.

8.3.2 Failure in a Certificate Authentication Check

Consider another scenario where a trading software check in step 5 in Section 5.5.3.2(A) finds that a copy of the certificate presented by a trader who multicast a proposal to exclude another trader from the trading forum membership, is recorded as "suspected compromised" in the local certificate repository. A physical meeting with that trader finds that his physical appearance is sufficiently different from the photo in the presented certificate. Thus, it is expected that the relying parties will ignore the exclusion proposal as the presented certificate should no longer be trusted and there is sufficient evidence that its sender is using a spoofed identity to send such a proposal. However, there could be parties who receive the exclusion proposal that do not have a copy of the actual party's certificate in their local certificate repository, or may have not received the notification about the theft of that certificate' private key yet. In this case, they may agree with the exclusion proposal, which could then result in an unfair exclusion to the target party.

However, if the relying parties who detect such a failure, multicast a warning or alert message as illustrated in Figure 8.3 to other traders in the trading forum, it could alert them to exercise caution and take the necessary actions when they receive an exclusion proposal from the same party. This could help to reduce the possibility for such an unfair exclusion.

Trading Group:	Easy e-Flea Market
Communication Scope:	Multicast to all members
From:	Smart Jane — Member since: January 01, 2013
Date Sent:	Saturday, August 17, 2013 11:00 am
Subject:	Failure of a check in authenticating a certificate.
Type of Failure:	A copy of the presented certificate in the local certificate repository is found to be recorded as "suspected compromised".
Concerning	Little Henry — Member since: October 30, 2013
Harm Done:	None
Occasion, Date and Place:	Proposal to exclude Fussy Tom (Cert05) from the trading forum membership; Friday, August 16, 2013 at Grill House Café, Paris
Description:	A certificate (Cert15) presented by a trader, Little Henry in his proposal to exclude Fussy Tom from the trading forum membership is found to be recorded as "suspected compromised". Physical appearance of the presenting party is sufficiently different from the photo in the presented certificate. Supporting evidence provided is insufficient.
Comment:	It seems that the presenting party and the owner of the existing certificate in my local certificate repository are not the same person.
Recommended Actions:	Save Cert15 and mark it as "suspected compromised" for future reference. Exercise caution if receive an exclusion proposal from the same party.
Attached Documents / Evidence:	Exclusion proposal, Cert05, Cert15.
Comment by: Little Henry	It was not me who sent the exclusion proposal. It was sent by other party using my certificate that has been compromised. Digital Signature: Little Henry
Author's Digital Signature:	Smart Jane

Figure 8.3: An example of a warning or alert message for a failure in a certificate authentication check

8.4 Discussion

This section discusses the responsibilities of a trader as an author or a relying party of a warning or an alert message.

8.4.1 Responsibilities as an Author

As an author of a warning or an alert message, traders should be aware of the following responsibilities when issuing such messages so that they won't create issues like libel risks and so on.

1) Ensure that there is adequate evidence or uncontestable facts that fraud is being attempted before issuing any warnings or alert messages.

2) Make sure the title and contents of the warning or alert message do not suggest anything that will lead to libel risks.

3) Do not use any words or terms that impute bad intentions or could lead other traders to wrong conclusions.

4) Avoid exaggerating any facts or evidence.

5) If possible, get a response from the target party about the issue being expressed in the alert message before multicasting it to other traders.

8.4.2 Responsibilities as a Relying Party

As a relying party, traders should be aware of the following responsibilities.

1) Forward a warning or an alert message to other traders only if convinced that fraud is being attempted, the identity of its source or author is verified, its content has not been altered and supporting evidence is available.

2) Ignore or discard any warnings or alert messages if the identity of its source or author cannot be verified, its content is suspected to have been altered, or supporting evidence is not available or insufficient or unsatisfactory.

3) Take into account any response from the target party which is included in the warning or alert message, before deciding to accept or ignore it.

8.5 Conclusion

This chapter discusses the importance of allowing traders to share their knowledge about suspected misbehaviour or malpractice with other traders in the trading system by using warnings or alert messages. Although there are advantages that can be obtained by sharing such knowledge, it may also raise further issues such as libel, as the warnings or alert messages could be circulated based on unsound suspicions, or be maliciously inspired.

Thus, this chapter proposes a security warning scheme that is framed in a reasonably neutral way so that ill-intentioned traders cannot easily use the warnings or alert messages to support malpractice and does not encourage traders to leap to wrong conclusions. With support from the identity support scheme, reputation system and group membership service, the aim of this security warning scheme is to improve the security of the trading system by allowing traders to share knowledge about potential threats or risks, so that they will be wary in relevant transactions. However, before deciding to circulate any warnings or alert messages, traders are expected to consider the prudence, ethics and legal implications of issuing such messages.

Chapter 9

Formal Verification of Ad Hoc M-commerce Trading Systems with SPIN

9.1 Introduction

The reliability of ad hoc m-commerce trading systems is important to increase users' confidence in the safety and correctness of the trading system. However, designing a reliable ad hoc m-commerce trading system is a challenging task. Such trading systems with complex processes may not function in an expected way or may be prone to failure due to common design flaws such as system deadlock, livelock and so on. For example, a trading request from a potential trader can be unexpectedly rejected due to these design flaws, resulting in that trader to lose an opportunity to engage in a particular transaction.

Thus, in order to ensure the reliability of an ad hoc m-commerce trading system, it is necessary to ensure that it satisfies enough system correctness properties. There are at least two categories of correctness properties that a system usually wants to satisfy, which are safety properties and liveness properties [13]. The safety properties assert that bad things should not happen, which means that a program should not enter an unacceptable state. The liveness properties assert that eventually something good happens, which means that a program eventually enters a desirable state.

One way to check whether the processes of an ad hoc m-commerce trading system satisfy its desired correctness properties is by performing formal verification of the system. A formal verification is a process of checking whether the design of a system satisfies certain requirements or properties. Thus, this chapter presents a formal verification of the processes of an ad hoc m-commerce trading system to ensure the reliability of the trading system, through an example of verifying the processes in one of its main trading steps using the SPIN model checker. However, it only concentrates on verifying certain safety properties of ad hoc m-commerce trading systems.

The remainder of this chapter is structured as follows. Section 9.2 discusses the method used for formal verification of ad hoc m-commerce trading systems. Section 9.3 specifies the processes involved in the formal verification of ad hoc m-commerce trading systems. Section 9.4 discusses how the specified ad an hoc m-commerce trading system processes can be translated into a PROMELA model. Section 9.5 specifies the safety properties to be verified and presents the verification results. Finally, Section 9.6 concludes this chapter.

9.2 Verification Method

There are several methods that can be used to verify the correctness properties of a system, which include simulation, testing, deductive verification and model checking [16]. Model checking seems to be the appropriate approach for ensuring the safety properties of ad hoc m-commerce trading systems due to its ability to easily deal with system properties such as safety and liveness properties. It provides an automated way to check whether a system satisfies certain properties, by building an abstract model of the system and exploring all of its possible execution paths.

To verify the safety properties of ad hoc m-commerce trading systems, the model checker SPIN will be used as a model checking tool.

9.2.1 SPIN

SPIN is one of the most prominent model checker tools that can be used for the formal verification of distributed and concurrent systems [75],[5],[141]. It is designed to perform model checking and simulation on a verification model of a system written in PROMELA (Process Meta-Language).

A PROMELA model consists of processes, message channels and variables. Processes are the system components that communicate with each other via message

channels and shared variables. With SPIN, the PROMELA models can be analyzed to verify the correctness of a system's behaviour or desired properties that are specified using LTL (Linear Temporal Logic) statements [141].

9.3 Ad Hoc M-commerce Trading Processes

To engage in ad hoc m-commerce transactions, traders must perform at least the following four main steps (the details of each step are discussed in Section 4.4):

Step 1 - Exchange trading standing

Step 2 - Agree a deal

Step 3 - Direct interaction to complete transaction

Step 4 - Exchange deal evaluations

However, as most of the main processes of an ad hoc m-commerce trading system occur during the exchange trading standing step, this thesis will use the processes in this step for the formal verification of an ad hoc m-commerce trading system. The processes include the PGP authentication process, membership voucher verification process and also reputation check process.

9.3.1 Exchange Trading Standing Processes

The exchange trading standing step is initiated when a trader receives a trading request together with a digitally signed trading standing from a potential trading partner. The digitally signed trading standing consists of the requested party's PGP certificate, membership voucher and a set of his recent deal evaluations and any testimonials that he has. The ad hoc m-commerce trading system will first check the validity of the presented PGP certificate through the certificate authentication process (Chapter 5). If the check is successful, it will then check the validity of the presented membership voucher through the membership voucher verification process (Chapter 7). If not, it will alert the trader with a failure notification. If both PGP certificate and membership voucher checks are successful, it will then evaluate the requested party's reputation (Chapter 6). If the result of the reputation checks is satisfactory, the trader will decide whether or not to enter into the transaction, after considering the potential transaction risks.

If the trader decides to proceed with the transaction, he will need to send an agree message together with his trading standing to the potential trading partner so that

he can perform the same process before they can proceed to ***agree a deal*** step. Otherwise, the trading request will be rejected and the process will be terminated.

Figure 9.1 illustrates how the processes in the exchange trading standing step can be modeled as a BPMN (Business Process Modeling Notation) diagram [6]. The model is presented as a BPMN diagram because it provides a standard, easy to define and also understand the core elements in a business process, which is required to specify the processes involved in the Exchange Trading Standing step.

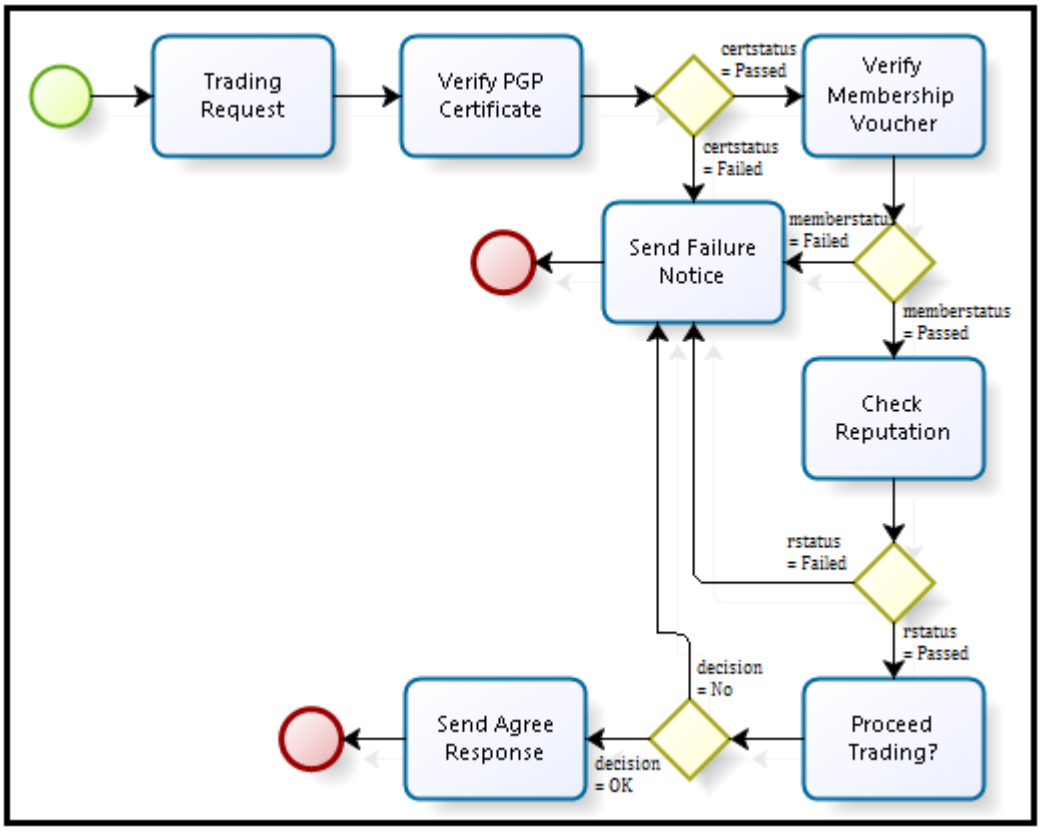


Figure 9.1: A BPMN model for the exchange trading standing processes

9.4 The Promela Model

This section will specify the activities involved in the exchange trading standing process as a PROMELA model. In this PROMELA model, six (6) global channels (denoted by the array of channels **ch**) are required to allow communication between two given activities, for example, channel ch[0] is used to establish communication between **Trading Request** activity and **Verify PGP Certificate** activity.

Trading Request - This activity is initiated by receiving a request from a potential trading party for a trade and is translated into the PROMELA process ***tradingRequest*** as follows:

```
proctype tradingRequest( )      /* A trader request for a trade */
{
    ch[0]!1;
}
```

Verify PGP Certificate - This activity will check the validity of a PGP certificate sent by the requested party (the details of the PGP certificate checks are discussed in Chapter 5) and it has to choose one of the two possibilities; whether to activate the ***verifyMembership*** process or ***sendFailurenotice*** process, depending on the result of the check. This activity is translated into the PROMELA process ***verifyCert*** as follows:

```
proctype verifyCert(mtype certstatus)
{ int x;
    ch[0]?x;                    /* To receive from tradingRequest */
    if
        :: certstatus == Passed ->ch[1]!1; run verifyMembership(...);goto End;
        :: certstatus == Failed ->ch[2]!1; run sendFailurenotice(); goto End;
        :: else ->goto End;
     fi;
End: skip;
}
```

Send Failure Notice - This activity will be activated when the check done by the ***verifyCert*** or ***verifyMembership*** or ***checkReputation*** or ***proceedTrading*** processes fails. It will inform the trader to reject the trading request and terminate the process. This activity is translated into the following PROMELA process ***sendFailurenotice***:

```
proctype sendFailurenotice()
{ int y;
    ch[2]?y;                /* To receive from verifyCert or VerifyMembership
                               or checkReputation or proceedTrading */
}
```

Verify Membership Voucher - This activity will check the validity of a membership voucher of the requested party (the details of the membership voucher checks are discussed in Chapter 7) and it has to choose one of the two possibilities; whether to activate the ***checkReputation*** process or ***sendFailurenotice*** process, depending on the result of the check.

It is translated into the PROMELA process ***verifyMembership*** as follows:.

```
proctype verifyMembership(mtype memberstatus)
{ int x;
   ch[1]?x;                 /* To receive from verifyCert */
   if
      :: memberstatus == Passed ->ch[3]!1; run checkReputation(...);goto End;

      :: memberstatus == Failed ->ch[2]!1; run sendFailurenotice(); goto End;
      :: else ->goto End;
    fi;
End: skip;
}
```

Check Reputation - This activity will check the reputation of the requested party and it has to choose one of the two possibilities, whether to activate the ***proceedTrading*** process or ***sendFailurenotice*** process; depending on the result of the reputation check. It is translated to the following PROMELA process ***checkReputation***:

```
proctype checkReputation(mtype rstatus)
{ int x;
  ch[3]?x;                    /* To receive from verifyMembership */
  if
    :: rstatus == Passed ->ch[4]!1; run proceedTrading(...);goto End;
    :: rstatus == Failed ->ch[2]!1; run sendFailurenotice(); goto End;
    :: else ->goto End;
  fi;
End: skip;
}
```

Proceed Trading - This activity will inform the trader that the PGP certificate, membership voucher and reputation checks are successful. The trader can then choose one of the two possibilities; whether to accept or reject the trading request. It is translated to the PROMELA process ***proceedTrading*** as follows:

```
proctype proceedTrading(mtype decision)
{ int x;
  ch[4]?x;                    /* To receive from checkReputation */
  if
    :: decision == OK ->ch[5]!1; run sendAgreeresponse(); goto End;
    :: decision == No ->ch[2]!1; run sendFailurenotice(); goto End;
    :: else ->goto End;
  fi;
End: skip;
}
```

Send Agree Response - This activity is activated by the activity ***Proceed Trading*** and will inform the trader to proceed with the trading by sending an agree message to the requested party.

proctype sendAgreeresponse()

{ int x

ch[5]?x; */* To receive from proceedTrading */*

}

Below is the corresponding PROMELA model description that is translated from the BPMN diagram in Figure 9.1.

mtype = {None, Passed, Failed, OK, No};

chan ch[6] = [1] of {int};

proctype tradingRequest() {...}

proctype verifyCert(mtype certstatus) {...}

proctype sendFailurenotice() {...}

proctype verifyMembership(mtype memberstatus) {...}

proctype checkReputation(mtype rstatus) {...}

proctype proceedTrading(mtype decision) {...}

proctype sendAgreeresponse() {...}

init { atomic { run tradingRequest(); run verifyCert(Passed); } }

9.5 Properties Verification

To ensure that the processes of an ad hoc m-commerce trading system satisfy certain safety properties, this thesis will consider the following properties to be verified using the SPIN model checker:

1. The first property to be verified is whether the processes in the exchange trading standing step are free from system deadlock. System deadlock is one example of the default system safety properties. It is a situation in which two competing processes are each waiting for the other to complete before proceeding, resulting in both processes ceasing to function. To verify this property, the setting parameter within the "Safety" panel in the SPIN model checker tool (iSpin) is set to "invalid end state (deadlock)". This will check if there is any process that does not reach the end of its code upon termination (invalid end state). If there is any process

found to be in that state, an error will be reported. This indicates that there is a system deadlock.

However, the output within the verification result panel shows that the verification is successful (no errors found), as as illustrated in Figure 9.2. This shows that every instantiated process is in a valid end-state and thus, it verifies the absence of system deadlock.

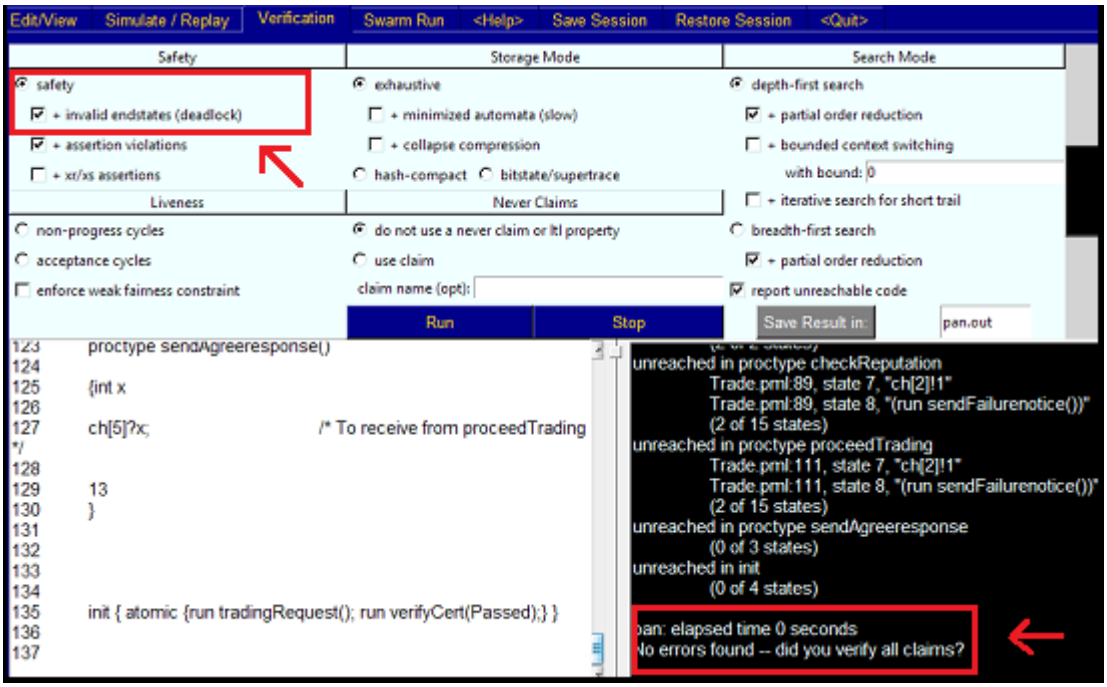


Figure 9.2: Verification result for deadlock freedom properties

2. The second property to be verified is that the trading request process will never accept and reject the same request. To express this property, a global *bool* variable *trade* is used and the following definitions are made:

   #define start (trade==false) ; /* when the process starts */

   #define accept (trade==true); /* before activity *sendAgreeresponse* ends */

   #define reject (trade==false); /* before activity *sendFailurenotice* ends */

   This property is then expressed in LTL as follows:

   ! (<>(accept && reject))

   To verify this property, the setting parameter within the "Never Claims" panel is set to "use claim". This will check if the never claim statement is matched. If it is matched by any system execution, then an error will be reported.

   The result of the verification shows that there is no error found, as illustrated in Figure 9.3. This indicates that this property is successfully verified.

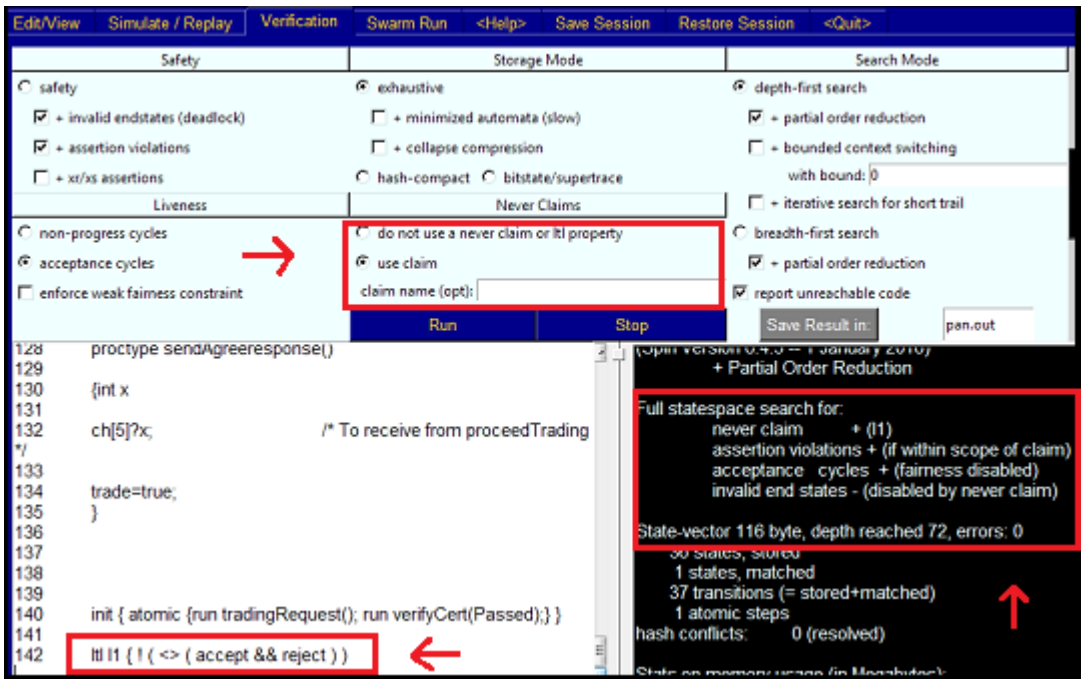


Figure 9.3: Verification result for second property

3. The third property to be verified is that whenever the trading request process is invocated, the process will either accept or reject the request. This property can be formally expressed in LTL as follows:

   [ ] (start -><>(accept || reject))

   Similar to the second property, to verify this property, the setting parameter within the "Never Claims" panel is set to "use claim". The verification result shows that there is no error reported, as illustrated in Figure 9.4, which indicates that this property is successfully verified with SPIN.

4. The fourth property to be verified is that it is impossible for a trading request to be accepted unless the checks on the requested party's PGP certificate, membership voucher and reputation are satisfactory. To express this property, the following definitions are added:

   #define cert_OK (trade==true) ; /* if certificate check passed */

   #define member_OK (trade==true) ; /* if membership check passed */

   #define reputation_OK (trade==true) ; /* if reputation check passed */

   This property is expressed in LTL as follows:

   [ ] (! accept U (cert_OK && member_OK && reputation_OK))

   To verify this property, the setting parameter within the "Never Claims" panel is again set to "use claim". The result of the verification shows that this property is also successfully verified, as illustrated in Figure 9.5

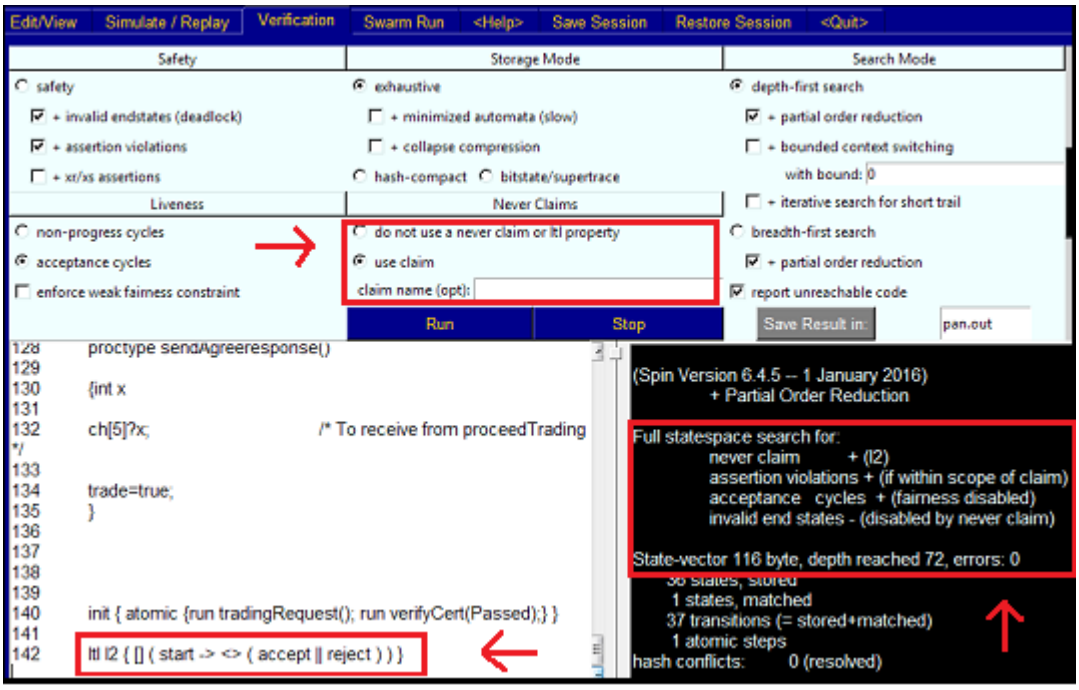


Figure 9.4: Verification result for third property

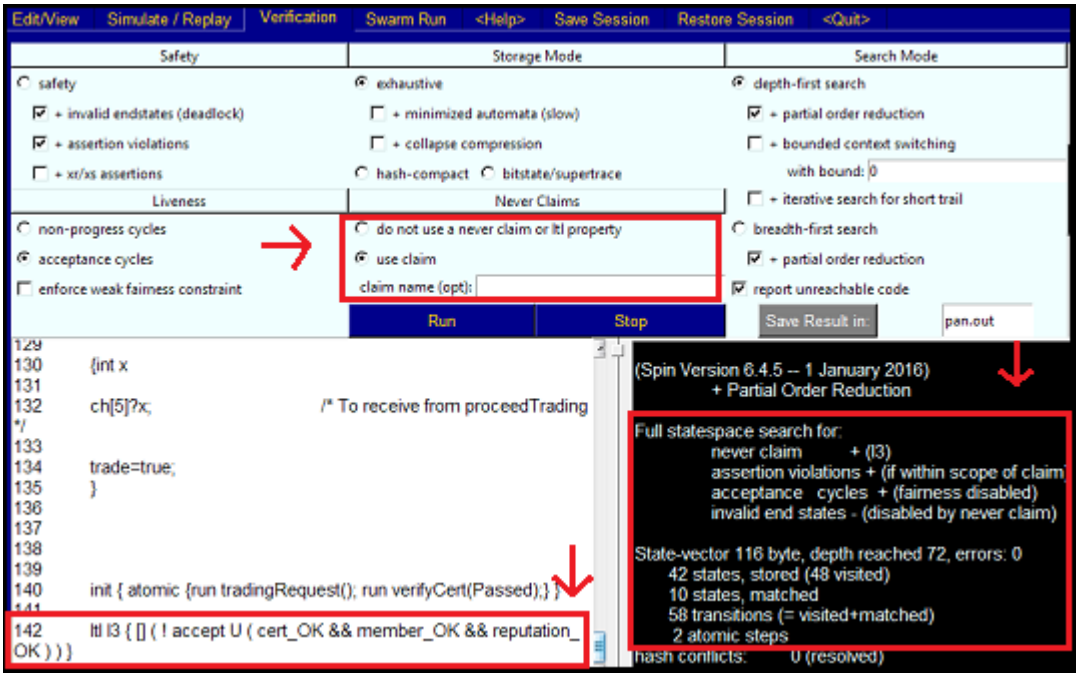


Figure 9.5: Verification result for fourth property

9.6 Conclusion

This chapter has presented an approach to verify certain safety properties of ad hoc m-commerce trading systems, by performing a formal verification of the processes of its exchange trading standing step using the SPIN model checker. It has discussed how the activities involved in the exchange trading standing step can be translated into a PROMELA model. It also has specified several safety properties to be verified and discussed how the specified safety properties can be expressed in LTL statements.

The model checking with SPIN verifies that the ad hoc m-commerce trading system is free from system deadlock and satisfies the other specified safety properties.

Chapter 10

Conclusions

This chapter discusses this thesis. Section 9.1 summarizes the entire research work. Section 9.2 discusses the limitations of this research work. Finally, Section 9.3 outlines the future works that can be done to extend or improve this research work.

10.1 Summary

This thesis concludes that ad hoc m-commerce is a new paradigm for conducting m-commerce wirelessly outside established computer networks and in a pure P2P architecture. It has argued that reliable security services can be supported under its constraints which can enforce security to a sufficient degree for trading to be viable using it. In that way it shows that ad hoc m-commerce is a viable alternative for mobile e-commerce to standard Internet m-commerce.

Although security analysis of the proposed security services shows that they have a useful effect in limiting the potential risk and impact of many kinds of fraud and cheating, they cannot stop fraud and cheating in such a loose ad hoc trading community. Thus, similar to non-digital marketplaces where traders are usually wary when dealing with unknown parties, traders in an ad hoc m-commerce also need to be wary and on the alert in each of their transactions.

10.1.1 Research Challenges

The current implementation of m-commerce predominantly utilizes infrastructure-based architectures (client/server and hybrid P2P based architectures), where users make use of a pre-established infrastructure supported by a network service provider. These kind of architectures are relatively stable, easy to implement and able to sup-

port a wide range of users and businesses that are located locally or globally. These architectures usually have better security as they can rely on the security services provided by a network service provider. However, although there are a variety of wireless communication standards that can be used by the users to participate in infrastructure-supported m-commerce, network connectivity cannot be guaranteed in some places especially in rural areas, and users often have to pay subscription fees in order to get connected to the network.

An ad hoc architecture has rival attractions by providing a more convenient, flexible and low cost way of enabling m-commerce. With the advancement of mobile devices that are getting smaller, have longer lasting batteries and more functions, and also a rapid improvement in wireless communication technologies, there is a growing potential for this kind of architecture to be an interesting alternative for traders to perform m-commerce trading. However, the process of designing and developing ad hoc m-commerce services and applications is inherently more complex and challenging, as compared to infrastructure-supported m-commerce. This is due to the fact that they are executed on resource constrained devices and in an environment that is dynamic and cannot rely on any infrastructure support from a network service provider or any authority higher than a peer. Thus, careful consideration is required when designing and developing its supporting services especially with respect to security.

10.1.2 A Novel Design Framework for Ad hoc M-Commerce Trading Systems

Chapter 4 of this thesis proposes a novel framework for m-commerce trading that is conducted online and wirelessly outside established computer networks. It has features and characteristics for pure P2P m-commerce. It defines a standard trading model for an ad hoc m-commerce trading system and presents an abstract architecture for an ad hoc m-commerce trading peer that specifies the services required to support the core functionality of the trading system. In this framework, the ad hoc m-commerce transactions involve only two main entities (buyers and sellers) that are peers with a similar role. These two entities communicate and cooperate with each other using their available resources to carry out m-commerce transactions and also handle the security services of the trading system without relying on any infrastructure support from a mobile network operator.

To suit the nature, characteristics and security requirements of an ad hoc m-commerce trading system, this framework addresses the identified threats in the following ways:

- **Online Identity Establishment** - A PGP web of trust scheme is adopted to let the traders of an ad hoc m-commerce trading system establish their online identity in a fully self-organised manner, without any mediation of a CA. The scheme uses a trading pseudonym and a photograph as identity credentials in a PGP certificate.

- **Trust Establishment** - A fully distributed reputation system is adopted to allows traders to share their trading experience with their peers, in order to foster trust among them.

- **Attestation Mechanism** - The attestation mechanism is used as a means for traders to vouch for the validity of other traders' identity credentials, membership status and reputation.

- **Group Membership Management** - The ad hoc m-commerce trading system framework employs group membership as a means to constrain the trading system's participation to only parties that are regarded as reasonably trustworthy by their peers.

- **Sanction-backed Mechanism** - A sanction-backed mechanism is incorporated in the reputation system as an incentive for traders to behave in a proper manner especially in fulfilling their transaction agreement and providing truthful deal evaluations and testimonials.

- **Security Warning Scheme** - A security warning scheme is used as a means for traders to report and disseminate suspicious behaviour or suspected security violations in the trading system.

10.1.3 Thesis Achievements

This thesis makes the following research contributions:

I. A novel reference model for ad hoc m-commerce has been developed. This reference model establishes the concept of ad hoc m-commerce and identifies the characteristics, requirements, main entities and key functional components of an ad hoc m-commerce trading system. It also outlines the key issues that need to be addressed in order to realise such a trading system practically. This reference model is useful to help future researchers to have a better understanding of the nature of an ad hoc m-commerce trading system, as well as to grasp the key issues involved in such trading. (Chapter 2)

II. A threat model for an ad hoc m-commerce trading system has been defined. The threat model identifies potential threats and vulnerabilities that could subvert the functionality of an ad hoc m-commerce trading system and classifies them into three main categories, namely identity related-threats, information-related threats and misbehaviour related-threats. The threat model also identifies three key security requirements for the design of the security services for an ad hoc m-commerce trading system, namely constraining participation, sharing trading experience and sharing expressions of trust. Possible countermeasures to address or mitigate each category of threats have been identified, studied and critically analysed. In addition to that, the ways in which the appropriate countermeasures can be modified and implemented to suit with the security requirements, as well as the nature and characteristics of an ad hoc wireless network have been studied, analysed and evaluated. (Chapter 3)

III. A novel framework for an ad hoc m-commerce trading system has been formulated. This framework defines a standard trading model for an ad hoc m-commerce trading system and an abstract architecture that specifies the core services that are required to support the functionality of the trading system. It addresses the identified threats in a way that is suitable to the nature, characteristics and security requirements of an ad hoc m-commerce trading system. Compared with infrastructure-supported m-commerce architectures, the ad hoc m-commerce framework provides several advantages in terms of providing a more convenient, flexible and low cost way of building m-commerce. (Chapter 4)

IV. A novel identity support scheme for a security and trust service in an ad hoc m-commerce trading system has been designed and evaluated. This scheme is designed to allow traders to collaborate with each other to establish their online identity using PGP digital certificates and handle the attestation and authentication processes of those certificates in a fully self-organised and P2P manner, without any mediation of a CA. A security analysis is given on the proposed design to show that appropriate checks on a trader's PGP certificate in the certificate attestation and authentication processes can help traders to detect misrepresentation of identity credentials in a PGP certificate in a significant number of scenarios, or at least be alerted that further checks are required to verify the validity of such certificates. (Chapter 5)

V. A fully distributed reputation system with high availability, efficient retrieval and reliable reputation information has been designed and evaluated. A security analysis is given on the proposed design to show that it can help traders detect or mitigate the identified misbehaviour-related threats to a sufficient degree. (Chapter 6)

VI. A novel group membership service for constraining traders' participation into an ad hoc m-commerce trading system has been designed and evaluated. Based on the security analysis that has been given on the proposed design, it shows that appropriate checks on a trader's membership voucher and votes can mitigate the major threats except for those involving extensive collusion among enough parties to meet the trading forum's membership support requirements. (Chapter 7)

VII. A security warning scheme to improve the security of an ad hoc m-commerce trading system has been proposed. This scheme is designed to alert traders about potential threats or risks in their transactions. (Chapter 8)

VIII. An ad hoc m-commerce trading model that satisfies certain system safety properties. A formal verification using the SPIN model checker verifies that the processes of an ad hoc m-commerce trading system satisfy the specified safety properties, including the deadlock-freedom property. (Chapter 9)

Table 10.1 summarizes the objectives and achievements of this research.

Research Objectives	**Outcomes**
Objective I	***Achievement I*** A novel reference model for ad hoc m-commerce
Objectives II, III and IV	***Achievement II*** A novel threat model for ad hoc m-commerce
Objective V	***Achievement III*** A novel framework for ad hoc m-commerce
Objective VI	***Achievement IV*** A novel identity support scheme for ad hoc m-commerce ***Achievement V*** A fully distributed reputation system for ad hoc m-commerce ***Achievement VI*** A novel group membership service for ad hoc m-commerce ***Achievement VII*** A security warning scheme for ad hoc m-commerce
Objective VII	***Achievement VIII*** An ad hoc m-commerce trading model that satisfies the specified safety properties

Table 10.1: Summary of the objectives and achievements of the research

10.2 Limitations

This research work has some limitations, which include the following:

I. The proposed design of security services only addresses or proposes to mitigate the most relevant threats in an ad hoc m-commerce trading system, which include identity-related threats, information-related threats and misbehaviour related threats. Other possible threats arising in relation to the perversion of the code of ad hoc m-commerce applications, subverting the confidentiality of network communications and compromising the physical security of mobile devices are not yet addressed or considered.

II. Only two of the core services that are required to support the functionality of an ad hoc m-commerce trading system, which include a security and trust service, and membership service have been designed and evaluated, but not yet implemented. Other core services remain to be designed, implemented and evaluated, such as discovery service, messaging service and forum decision making service.

III. The effectiveness of the proposed design of the security and trust service, and also membership service in addressing the identified threats has been evaluated based only on an informal proof of security, where the means by which the reliability of such services can be compromised by ill-intentioned parties were critically analysed and reviewed. Although this kind of security evaluation has purported to show that such security services are able to detect and address nearly all of the identified threats to a sufficient degree, it would be more credible if a security validation based on experience with a concrete realisation of an ad hoc m-commerce trading system framework could be carried out to demonstrate that such security services are able to support the security of a real ad hoc m-commerce trading system, as well as to identify flaws and weaknesses in their design components. However, as a full prototype of ad hoc m-commerce applications has not yet been developed, it is infeasible to carry out such a security validation.

IV. The proposed design of the identity support scheme has several limitations. The software checks in both the certificate attestation and authentication processes can only detect misrepresentations of identity credentials in a presented PGP certificate if a copy of that certificate and/or its signatories' certificates are available to the user. Also, such checks can only detect attempts by ill-intentioned parties to create multiple identities or re-enter the trading system with a new identity if the copy of the certificate for their other identities are available to the user. Although the trading software will alert traders to check

around that the party in question is known by his pseudonym and meet that party in person to verify his physical appearance if a copy of such certificates is not available locally, there is no guarantee that they will be able to obtain such information and/or detect that the presenting party is not the real owner of the presented certificate, or has other identities. This is because the other trusted parties also may not have the copy of the certificates or they may not be available during the period when such information is required. In addition to that, the traders might not be suspicious of the validity of the presented certificate if the real physical appearance of the presenting party shows some or a clear resemblance to the photo appearance in the presented certificate. However, such an alert from the trading software will help to reduce the likelihood of a successful attempt.

V. As the design of a fully distributed reputation system for an ad hoc m-commerce trading system only aims at providing an effective way to facilitate trust development among traders by addressing the three key design issues as discussed in Section 6.3, there is no complete scheme for evaluating deals that considers the nature and characteristics of an ad hoc m-commerce trading system, as well as the limited capabilities of mobile devices has been designed and implemented.

VI. A prototype for any of the potential ad hoc m-commerce applications has not yet been developed. The development of such a prototype would require other core services such as a discovery service, messaging service and a forum decision making service to be designed and implemented first in order for an ad hoc m-commerce trading system and its security services to be fully functional. It would be the first step towards a realization of ad hoc m-commerce trading systems in the real world. Such a prototype could be used to provide concrete experience of conducting ad hoc m-commerce trading in order to evaluate the effectiveness of the proposed approach of its core services, as well as to discover other as yet unanticipated possible threats or vulnerabilities in such a trading system.

10.3 Future Work

There are several ways to extend or improve this research and address the limitations identified in Section 9.2.

I. To complete the implementation of the security services for an ad hoc m-commerce trading system by addressing other possible threats which relate to the perversion of the code of ad hoc m-commerce applications, network

communications and compromised of the physical security of mobile devices. This would improve the security of an ad hoc m-commerce trading system.

II. To complete the implementation of an ad hoc m-commerce trading system framework. This might be achieved by designing and implementing the other core services which include the discovery service, messaging service and also forum decision making service. These services are important to enable the traders of an ad hoc m-commerce trading system to communicate and collaborate with each other in order to participate in m-commerce transactions and also handle the security services of the trading system.

III. To address the limitations of the proposed identity support scheme. This might be achieved by investigating approaches to improve the PGP certificate attestation and authentication processes and make the process of sharing expressions of trust among traders in such a loose and dynamic trading system more effective and reliable.

IV. To design, implement and evaluate a more appropriate scheme for evaluating deals for a fully distributed reputation system for an ad hoc m-commerce trading system. The scheme should be at least simple to understand, quick to use, able to clearly differentiate out different quality aspects and suitable to be used on resource constrained mobile devices.

V. To develop a complete prototype of a specific ad hoc m-commerce application so that the functionality and viability of such a trading system can be tested and the effectiveness of its security services and other core services can be validated based on concrete experience with the prototype in a more realistic scenario.

VI. To explore other methods of security validation for a more convincing result and more credible proof of security. For example, to engage hostile security experts to do sceptical reviews or give critical evaluations based on their experience with a concrete implementation of the ad hoc m-commerce trading system prototype.

VII. To address the other issues at stake that might restrain the development of an ad hoc m-commerce trading system in order to realise it practically in the real world, such as mobile device issues, ad hoc wireless network issues, transaction management issues and so on.

Appendix A

Published Paper: Towards a Reference Model for Ad Hoc M-commerce

Towards a Reference Model for M-Commerce over Ad Hoc Wireless Networks

Husna Osman, Hamish Taylor

Abstract — Wireless trading outside established computer networks is an emerging class of mobile application for which there seems to be a growing demand. It enables mobile users to wirelessly engage in online trading regardless of time or location. However, better understanding of the complex issues at stake is needed before effective systems of this kind can be designed and built. Developing a reference model is one way to provide this understanding. M-commerce is defined and its elements, requirements and issues are discussed. The characteristics, functional components, application types, security requirements and issues of ad hoc m-commerce are then analyzed and distinguished.

Index Terms — e-commerce, mobile computing, spontaneous dealing, wireless trading.

1 INTRODUCTION

Performing m-commerce transactions over ad hoc wireless networks or ad hoc m-commerce can be considered as wireless trading outside established computer networks. It enables users to engage in m-commerce transactions by using computing resources on nearby devices without the need for infrastructure support from a network service provider [1].

However, to make ad hoc m-commerce a reality, it is important to clearly understand ad hoc wireless networking as well as m-commerce concepts, requirements and challenges. Therefore, having a reference model should help to grasp the key issues involved in trading wirelessly among computing nodes in the absence of a network service provider. It will facilitate discussion on distinguishing aspects and issues of ad hoc m-commerce as well as be useful in identifying and facilitating Research and Development (R&D) for a wide range of ad hoc m-commerce applications. A reference model will:

1. Establish a taxonomy of terminologies, concepts and definitions required for describing ad hoc m-commerce.
2. Identify all the functional elements in ad hoc m-commerce systems and clarify dependencies among them.
3. Identify any issues that might restrain the development of ad hoc m-commerce that need to be addressed to realise it practically.

Hence, this paper proposes the elements of an ad hoc m-commerce reference model to serve as a basis for understanding the nature as well as the requirements for performing such trading. The rest of this paper is structured as follows. Section 2 discusses the nature of m-commerce, its functional components and also requirements. Section 3 discusses several essential m-commerce issues in detail. Section 4 describes ad hoc m-commerce and discusses its specific issues and possible applications. Section 5 concludes the paper.

2 M-COMMERCE

2.1 M-Commerce Definition

The term m-commerce has been defined in a variety of ways in different literatures [2],[3],[4],[5]. Some of these definitions seem to restrict m-commerce to business transactions that are conducted solely over a mobile telecommunication network and involve the transfer of monetary values. However, m-commerce transactions do not necessarily involve the transfer of money and can be conducted over other means of wireless communication. Furthermore, all commercial transaction steps need not be carried out electronically. While some transactions are initiated and completed electronically, some transactions may be initiated electronically but completed off-line.

Therefore, in this paper, m-commerce is defined as a set of activities relating to the exchange of information, services and goods for either money or other information, services and goods, which is conducted fully or partly online over wireless technology using mobile devices. In a fully online transaction, all transaction processes, which include the advertising, negotiating, ordering, payment and delivery processes, are conducted electronically. In a partly online transaction, the transaction may be initiated

electronically but not completed electronically. Steps like the advertising, negotiating and ordering processes may be done online but other steps like payment and delivery processes may be done off-line.

M-commerce has several unique characteristics. Based upon different literatures [6],[7],[8] m-commerce's distinguishing characteristics can be summarized as follows:

1. Location and Motion Independence
   The portability of mobile devices, the pervasiveness of mobile network access and widespread m-commerce service availability makes m-commerce transactions possible irrespective of where the user is or whether the user is moving.
2. Localizability
   Technologies like Global Positioning System (GPS) enable users and mobile network operators to locate each other and to make access to commerce services specific to their location.
3. Personalisation
   Mobile devices are usually not shared among users. This enables users to customise these devices to their individual commerce service requirements.

2.2 M-Commerce Functional Components

M-commerce systems involves various disciplines and technologies [9]. In order to have a clear understanding of m-commerce systems, it is essential to identify their components as well as to recognize their functions and dependencies with one another. We follow [9] in dividing m-commerce systems into six components.

1. Mobile Commerce Applications
   There are a wide variety of existing and potential m-commerce applications. These applications can be classified into several classes as listed in table 1.

TABLE 1
CLASSES OF M-COMMERCE APPLICATIONS

Class of Applications	Examples
Information	News and Weather Maps and travel related information Logistical information Emerging service information
Entertainment	Sports, Games and Gambling e-Books, e-magazines Movies, images and music Streaming media
Financial	Banking Mobile Auctions Booking and Reservation Online shopping and stock trading
Marketing and Advertising	Mobile coupons and promotions

2. Mobile Stations or Devices
   Mobile devices with sufficient power in terms of memory, display and communications functionalities enable consumers to engage in m-commerce transactions regardless of time or location.
3. Mobile Middleware
   Mobile middleware can be defined as an enabling layer of software that joins together different mobile applications, networks and technologies via a common set of interfaces [10]. It enables m-commerce applications to function with greater reliability as well as to provide better response times.
4. Wireless Networks
   In addition to mobile devices and middleware, networking support from wireless networks plays an essential role in realizing m-commerce applications. Wireless networking technology available to support m-commerce includes operator-driven networks like GPRS and UMTS, wireless LAN via Wi-Fi (Infrastructure and Mobile Ad Hoc Wireless Network) and wireless PAN via Bluetooth.
5. Wired Networks
   Although this component is an option, most computers or servers that are used to execute transaction processes and store all the transaction information usually reside on wired networks.
6. Host Computers
   Host computers are used to process and store m-commerce transaction related information such as Web servers and database servers.

2.3 Main Entities in M-Commerce System

Generally, there are four main entities in m-commerce systems [11].

1. Customer
   The person who is mainly mobile and makes use of the m-commerce system for the purpose of obtaining and paying for contents, products or services offered by merchants or content/service providers.
2. Merchant or Content/Service Provider
   The entity that provides the contents, products and services to customers either directly or through a mobile network operator.
3. Mobile Network Operator
   The entity that provides the network connectivity that links customers, merchants and financial institutions.
4. Financial Institution

The entity that provides the payment mechanism such as EFTPOS or ATM service.

2.4 Entities Relationships in the M-Commerce Value Chain

Entity relationships in an m-commerce value chain can vary depending on the types of transactions. For example, a relatively simple transaction such as buying a soft drink from a vending machine would only involve a customer, mobile network operator and its vending machine that supplies soft drinks [11]. In this scenario, the customer has relationships with both the mobile network operator and the vending machine. The mobile network operator charges the customer for using its service to purchase the soft drink by adding the cost of the soft drink to the customer's mobile phone bill.

A more complex m-commerce transaction might involve a financial institution. In this scenario, the customer has a relationship with the mobile network operator, the financial institution and also the merchant [11]. The mobile network operator enables the transaction to take place by providing mobile services to the customer. To purchase products, the customer needs a relationship with the financial institution that handles the transaction payments. The customer will also need a relationship with the merchant for the goods purchased.

Another scenario is a relationship between a customer and mobile network operator and also a relationship between a network operator and content provider [12]. The customer obtains the content or service from its provider through its mobile network operator and pays the operator who remunerates the content or service provider in turn.

2.5 M-Commerce Requirements

Although different m-commerce applications have different requirements, in general m-commerce applications have the following requirements:

1. Adequate quality of service in the wireless network to avoid delays that may affect the performance of m-commerce applications.
2. Reliability in the wireless network so that users can access m-commerce applications, even under varying degrees of network failure.
3. Ability to roam across multiple heterogeneous networks so that users can access m-commerce applications from anywhere.
4. End-to-end security supported so that trading parties can trust the other trading parties to provide their service at an acceptable level of risk.
5. Convenience and usability so that users can perform m-commerce transactions easily and unproblematically.

3 M-COMMERCE ISSUES

3.1 Mobile Devices

Mobile devices have limitations in terms of battery life, resources and display capabilities.

1. Battery life
   Mobile devices have limited battery lifetimes during which they can operate without recharging their energy resources. This limitation restricts mobile devices from performing much complex and energy intensive computations. Moreover, the use of a wireless medium for data transmission can make the battery life shorter as it consumes significant energy [3]. Therefore, mobile devices cannot be expected to be always available in a network like stationary computing devices. Users may cut their wireless connection to the network to reduce power consumption or the battery may suddenly become flat.
2. Limited resources
   Mobile devices have limited resources in terms of CPU capacity, storage capacity and processing space due to their small size and portability. These limitations restrict the amount of computation performed and also the amount of data stored on these devices.
3. Small screen and keypad
   The small screens and limited text input capabilities of mobile devices limit the size of information that can be displayed and make data entry more difficult. Also, they limit capabilities for use of high quality graphics [3].

3.2 Wireless Networks

Wireless networks have limited bandwidth. Although they may come to have higher bit rates, the transmission rates in many wireless networks such as in cellular or satellite networks are still low as compared to wired networks [3]. This is partly because wireless communications are rather more error prone and require much redundancy in the channel coding of the payload [3].

In addition to that,wireless networks are

less reliable due to frequent network disconnections. Factors that cause network disconnections include lack of network coverage, cell interference, changes in the signal strength and limited battery lifetime of mobile devices. In some m-commerce applications such as online trading or entertainment, continued network connectivity is an important requirements as discontinued connections may affect the result of transactions.

Furthermore, channels in wireless networks may be asymmetric [13]. The bandwidth available for uploading data may be rather lower than the bandwidth available for downloading data.

Also, different networks have different network access charges. In some networks, access is charged per connection-time for example in cellular telephones, while in some others, it is charged per message or per session [3].

3.3 Security

There are at least three aspects of security that need to be considered: the security of mobile devices, the radio interface and payment systems.

1. Mobile devices
   Due to their small size and portability, mobile devices are prone to be stolen, lost or accidentally damaged. Since these devices are highly personalized and are often used to store confidential user information, it is important to protect not only the data that is transmitted through the network but also the data on the device itself. However, their limited computation capabilities and memory size make it difficult to use high level security schemes.
2. The radio interface
   Performing electronic transactions over wireless networks is inherently insecure as compared to wired networks [12]. A radio interface introduces additional security vulnerabilities. Its broadcast nature makes it easier for attackers to intercept and spoof on going traffic if no security mechanisms such as communication encryption are employed. There are three common types of attacks: disclosure attacks, integrity attacks and denial of service attacks [14]. Disclosure attacks are where the confidentiality of data transmitted over the network is compromised by its contents being revealed to other parties that are not involved in the communication by means such as eavesdropping, masquerading, traffic analysis and so on. Integrity attacks are where the contents of a message being transferred over the network is illegally altered or deleted or reused without permission. In a denial of service attack, access to the network is made impossible by flooding and overloading the network with messages. In addition to security attacks, frequent handoffs and disconnections due to path loss, fading and interference can degrade the service levels of security services. Also, the mobility of mobile devices introduces an additional difficulty in identifying and authenticating devices in the network.
3. Payment System
   M-commerce applications, especially those involving mobile payments require secure information exchange as well as safe electronic financial transactions. Without a secure payment system, neither customers nor merchants may be prepared to engage in monetary m-commerce transactions. For instance, both parties that are involved in a financial transaction would want to authenticate each other before committing to any payment. Also, they would want assurance on the confidentiality and integrity of the sent payment information as well as effective support for non-repudiation to prove that a transaction has happened.

3.4 Social, Ethical and Legal Issues

To avoid risks such as legal actions, brand infringement and so on, entities that are involved in m-commerce transactions must ensure that all m-commerce activities such as services, transactions, payments and so on, comply with government and industry regulations. Regulatory issues that need to be addressed include:

1. Data protection and data breaches
   Regulations related to the protection of subscriber data, identity theft and the reporting of data breaches.
2. Digital rights
   Digital content such as music, clip art, videos and so on are subject to intellectual property (IP) constraints such as copyright, trademarks and patents.
3. End-user privacy
   Regulations related to consumer protection and privacy laws to ensure consumer privacy is not violated.
4. Child protection

Regulations related to offering, accessing and purchasing of adult related content, products and services. Age verification may be required before any adult related content, products or services are obtained.

5. Money laundering and gambling
   Regulations related to electronic money transfers, money trafficking issues and so on.

4 M-COMMERCE OVER AD HOC WIRELESS NETWORKS OR AD HOC M-COMMERCE

Unlike infrastructure-supported m-commerce, ad hoc m-commerce takes place between 2 or more mobile devices that are peers and in the vicinity of each other. To accomplish a transaction, these devices communicate and cooperate with each other by utilizing their local resources and also their neighbours', without relying on any support provided by a network service provider. Thus, ad hoc m-commerce can be said to have the following characteristics:

1. No network service provider
   Because ad hoc wireless networks lack a network service infrastructure and are self-organized, a network service provider cannot be relied upon to be present to provide other security or payment services whenever nodes engage in m-commerce transactions.
2. Limited communications scope
   IEEE 802.11 (Wi-Fi) and Bluetooth have limited communication ranges [15],[16]. Therefore, such networks are suitable for short range node to node communication. While nodes can bridge gaps by routing information over multiple hops via nodes in between themselves and so extend the range of such networks, those ad hoc connections via intermediaries may not be long lasting and may not be available much of the time.
3. Limited time online
   Due to limited battery lifetimes and the mobility of mobile devices as well as frequent network disconnections, there is a limited time during which these devices can be online, which restricts them from engaging in lengthy and complex transaction processes. This means that transactions need to be completed in a fairly short period and only comprise a few simple stages if they are to have a good chance of success. Therefore, realistic transactions must not involve long sessions or complex processes. Since mobile devices are peers and these devices themselves can become the service or information provider as well as the consumer, the limited time online restricts a trusted service or information provider from providing ubiquitous services such as payment processing, or information such as a good trading history to other devices in the network.
4. Spontaneous decisions in Ad Hoc Settings
   The self-organizing characteristic of an ad hoc wireless network allows users that are equipped with mobile devices to spontaneously engage in m-commerce transactions when the need arises while they are on the move. For example, passengers in two cars near each other in slow traffic can establish an ad hoc wireless network connection and exchange video clips while within range of each other.
5. Low cost
   An ad hoc wireless network provides a low cost wireless connection for users to engage in m-commerce transactions. No additional device is required to perform ad hoc m-commerce as mobile devices that form the network will utilize their local resources and also resources on other devices in their proximity area in order to accomplish the transactions. The cost of purchasing or renting additional devices such as special server(s) that are used to process the transaction as well as to store transaction information is eliminated. Also, buyers or traders save on network access charges.
6. Confidentiality
   Because no third party needs to be involved to realise network communication, the range of wireless communication is limited, and can be conducted on the move, ad hoc m-commerce is suitable for confidential commercial exchanges where the trading parties do not wish their exchange to be known or guessed at by external parties. For example, two or more parties may exchange their confidential information while they encounter or merely pass close by each other.

4.1 Functional Components

Only the first four functional components discussed in section 2.2 may be required to construct an ad hoc m-commerce system because the network may be spontaneously and temporarily created when the need arises among mobile devices in close

proximity to each other. However, there is a slight difference in the fourth component where an ad hoc wireless network like mobile ad hoc network (MANET) or Bluetooth is used as a medium to carry out the transactions as shown in Fig. 1.

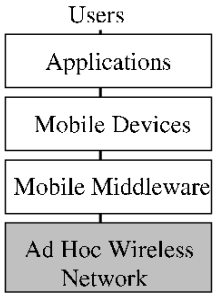


Fig.1. Four main functional components in an ad hoc m-commerce system.

Therefore, the design and development of m-commerce applications as well as mobile middleware must consider the unique characteristics of an ad hoc wireless network.

4.2 Main Entities

Since the transactions involve only mobile devices that are peers and have no guarantee of infrastructure support from a network service provider, there are only two essential entities involved in ad hoc m-commerce.

1) Customer or Trader
   The person who is mainly mobile and make use of the ad hoc wireless network to buy the digital contents, products or services offered by the seller or to trade contents, products or services for others.
2) Seller or Trader
   The person or entity that provides the digital contents, products or services directly to customers via ad hoc wireless networks for money or who trades contents, products or services for others.

Nevertheless, as different types of transactions would have different entity relationships, there are several possible essential entity relationships in the ad hoc m-commerce value chain. A relatively simple transaction might involve two mobile devices. For example, two people who are commuting in a train agree to exchange their e-magazines while they are within transmission range of each other. In a more complicated scenario where more than two mobile devices are involved in a transaction such as an auction, the entity relationship can be illustrated as below.

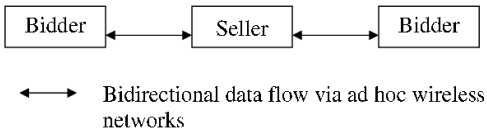


Fig.2. Transactions involving more than two mobile devices.

Fig. 3 and Fig. 4 illustrate two scenarios involving the formation of an ad hoc trading consortium among mobile users who are in the vicinity of each other and agree to band together for a specific purpose, for example to make a collective purchase (Fig. 3) or to engage in group trading (Fig. 4).

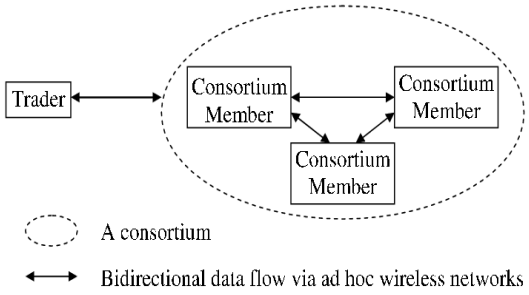


Fig.3. A group of individuals forming a consortium for trading.

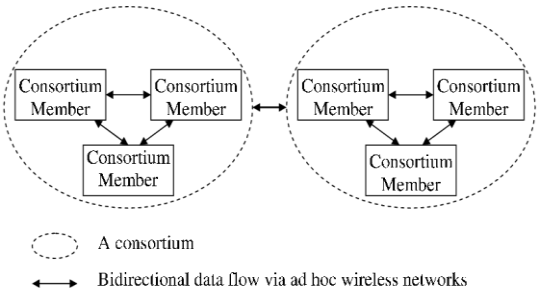


Fig. 4. Trading between two consortiums.

Fig. 5 shows a delegated trading scenario where an electronic I Owe U (IOU) is used to acknowledge debt between two parties trading via an ad hoc wireless network. It illustrates a scenario in a local community where Trader 1, who has a toaster, wants to trade it for an electric kettle. Trader 2, who is within Trader 1's communication range and owns an electric kettle, agrees to trade his electric kettle with Trader 1 but does not want a toaster. So, Trader 1 issues an electronic IOU signed by himself to Trader 2 as an acknowledgement of his debt to Trader 2. Trader 2 can later use that electronic IOU to trade for another item such as a pram that she wants with Trader 3, who wants a toaster. Trader 3 will then use the electronic IOU signed by both Trader 1 and Trader 2 to settle with Trader 1 for his toaster.

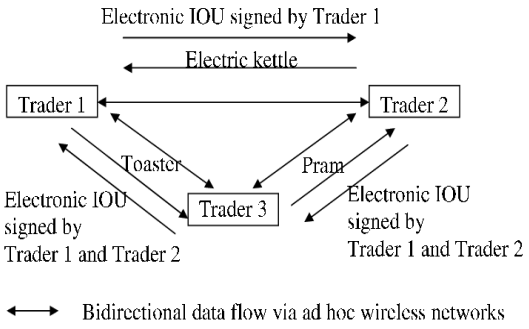


Fig. 5. A delegated trading scenario.

To represent various entity relationships in the ad hoc m-commerce value chain, a generic view of ad hoc m-commerce transactions is provided as Fig. 6.

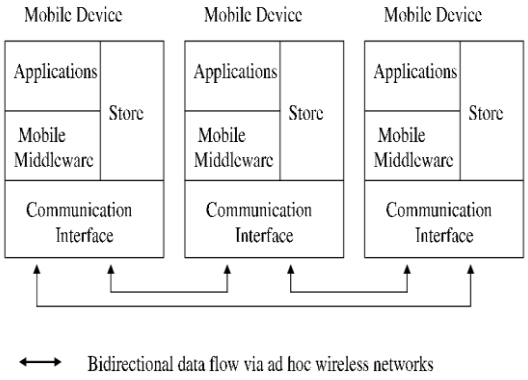


Fig. 6. A generic view of ad hoc m-commerce transactions. The ad hoc m-commerce store will held certificates, attestations, offers, IOUs, deals and so on.

4.3 Types of Applications

There are several distinct types of m-commerce transactions that can be carried out over ad hoc wireless networks:

1. Swapping of digital resources
   Swapping of digital resources such as ebooks, videos, music files etc. For example, two people who meet by chance at an airport may agree to exchange an MP3 pop song for an amusing video clip.
2. Mobile Auction
   The process of buying or selling certain items could be realised by an auction among a local group of people. An auction process can be created anywhere as soon as a group of at least three persons with mobile devices and shared software agree to participate. This type of activity is amenable to short term participation by individuals and a rapid turnover in its membership as long as enough are usually present to create a critical mass of bidders. Multicasting among participants can disseminate bids and information about what is on offer.
3. Mobile Entertainment
   Interactive gaming and gambling among small groups of people is another kind of application suited to ad hoc networking. Applications running on mobile devices realise the game or gambling scenario, manage its communications and handle the turnover in participants. For example, people play blackjack over a mobile ad hoc wireless network using mobile devices like laptop computers, PDAs or computers in cars.
4. Transacting with Machines
   Transactions that use mobile devices that are preloaded with E-cash to make payment at a vending machine, point of sales (POS), parking tolls and so on via technologies such as Wi-Fi and Bluetooth.
5. Confidential Exchanges
   Two or more parties who meet at a certain place or pass in the vicinity of each other may agree to exchange their confidential information resources or services for a specific purpose.
6. Consortium Trading
   A group of individuals who are in the vicinity of each other and equipped with mobile devices could spontaneously and temporarily form a consortium for a specific purpose. For example, a group of football fans at a football ground might band together as a single buyer to purchase a discounted group ticket in order to get a cheaper ticket for each of them to watch a match. Another example would be a group of football fans who form a consortium during a football match to engage in betting on the outcome with another group of football fans.
7. Electronic IOUs
   'I Owe U' or its abbreviation 'IOU' is an established means to acknowledge a small debt usually among friends or family members. This form of acknowledgement can be passed electronically via an ad hoc wireless network among trading parties. It can be signed to verify its authenticity and the identities of all handling parties.

4.4 Issues

Performing m-commerce transactions over ad hoc wireless networks introduces additional issues and challenges. In addition to the above issues, ad hoc wireless networks have specific issues that need to be considered. However, issues related to

variant tariffs are not applicable to ad hoc wireless networks as no access fee is required to access the network. Other issues that need to be considered when performing ad hoc m-commerce:

1. Transaction management
   Due to its nature such as lack of infrastructure, having a dynamic network topology and using resource constrained devices, it is a challenge to implement efficient transaction processing and updates in purely ad hoc wireless networks. Most solutions used in infrastructure based m-commerce depend on a client/server model where data is primarily placed on servers located within the wired network and mobile devices act as clients accessing the services provided by the servers [17]. However, in ad hoc wireless networks, all devices are peers and normally have similar constraints on their resources. Thus, those devices act as both servers and clients. The mobility of mobile devices that provide services (servers) to other devices is an important issue as the services are prone to becoming unavailable due to network disconnections. Also, the atomicity of a transaction can be difficult to enforce as network disconnections can cause a particular service in a transaction sequence to fail and thus the transaction would be considered incomplete and be aborted [17].
2. Service Discovery and Delivery
   A service discovery and delivery protocol enables devices to advertise their services to other devices as well as to discover services offered by other devices in the network. However, due to the unique characteristics and complexities of an ad hoc wireless network, existing service discovery and delivery protocols do not seem to suit the needs of an ad hoc wireless network, making them unsuitable for m-commerce oriented scenarios. Service advertisements and deliveries may need to be disseminated by a mix of a store and forward strategy as well as local multicasting to cope with intermittent online connectivity.
3. Trust
   Trust is essential in any online transactions as it helps the participating parties to feel confident enough to engage in such transactions by mitigating uncertainty and risks involved in the transactions, such as uncertainty about trading partners' behaviour in fulfilling the transaction agreements [18]. However, as ad hoc m-commerce cannot rely on a network service provider to provide security services such as certification authority (CA) that can help to establish trust among nodes in the network, nodes have to rely on their peers in the network to provide trust evidence in order to evaluate other nodes' trustworthiness. Yet, the nature of an ad hoc wireless network such as lack of infrastructure services, having a dynamic network topology, using resources constrained devices and so on, makes trust establishment in this network difficult to achieve.

4.5 Security Requirements

To create a sufficiently secure and trusted environment for a transaction to take place as well as to give confidence to trading parties to engage in a transaction, the following security services are essential.

1. Confidentiality
   Confidentiality ensures that transaction information sent across the network is unreadable by unauthorized third parties such as eavesdroppers or peers acting only as communication relays.
2. Authentication
   Authentication enables trading parties involved in m-commerce transactions to confirm the identity of each other before any transactions are made among them. This service provides assurance that an unauthorized third party is not masquerading as a legitimate party.
3. Integrity
   Integrity guarantees that a message being transferred is not illicitly altered or destroyed during the transmission without this being detectable at the receiving end of an m-commerce system.
4. Non-repudiation
   Non-repudiation ensures that if an entity sends a message, it cannot get away with denying having sent the message. In m-commerce transactions, neither sender nor receiver should credibly be able to repudiate offers or bargains struck between them. The sender should not be able credibly to deny having sent the transaction message and the receiver should be able to prove that the transaction message can only have been sent by the specified sender and thus able to prove that a

transaction has taken place between them.

In addition to the above, as m-commerce transactions involve the risk of misbehaviour among the trading parties, they need support in gauging the level of trustworthiness of other trading parties. Hence, attestation is another important security service for ad hoc m-commerce.

5. Attestation
   Attestation enables ad hoc m-commerce peers to vouch for the identity, trading history or transaction reputation of other peers. It helps mitigate risks in transacting with previously unknown parties.

5 CONCLUSION

An ad hoc wireless network can be an alternative to operator-driven GPRS/UMTS networks that provide networking support for m-commerce transactions, particularly in supporting spontaneous and low value transactions in ad hoc settings among unacquainted parties. It seems most suited to fully online resource swapping that does not require complex and lengthy processes and also to online launched trading in local communities where parties can easily meet to transfer goods and payment as agreed.

We believe that the elements of an ad hoc m-commerce reference model presented in this paper will be useful in designing and developing a wide range of ad hoc m-commerce applications and also valuable as a basis for future research in various aspects of ad hoc m-commerce. Our future work will be focusing on the issue of trust in ad hoc m-commerce. We will be developing a trust model that will enhance the security of an ad hoc wireless network as well as mitigate risks and uncertainties involved in the transactions, to make an ad hoc wireless network a sufficiently commercial secure and trusted medium for transactions to be able to take place. Simulation processes and experiments will be conducted to evaluate the effectiveness of the trust model.

ACKNOWLEDGMENT

The authors wish to thank the referees for their useful comments in improving this paper and also Dr. Peter King for his contributions to this research.

REFERENCES

[1] F. Perich, A. Joshi and R. Chirkova, “Data Management for Mobile Ad Hoc Networks,” *Enabling Technologies for Wireless e-Business Applications*, W. Kou & Y. Yesha, eds., Springer, 2005, pp. 1-37.

[2] J. Jonker, “M-Commerce & M-Payment: Combining Technologies,” [cited 20/06/08]; http://www.few.vu.nl/stagebureau/werkstuk/werkstukken/werkstuk-jonker.pdf. 2003, pp. 1-28.

[3] P. Tarasewich, R.C. Nickerson and M. Warkentin, “Issues in Mobile E-Commerce,” *Communication of the Association for Information Systems*, vol. 8, no. 3, 2002, pp. 41-46.

[4] M. Munusamy and H.P. Leang, “Characteristics of Mobile Devices and an Integrated M-commerce Infrastructure for M-commerce Deployment,” *Proc. 4th. Int Conf on Electronic Commerce*, 2002, pp. 1-10.

[5] J. Veijalainen, V. Terziyan and H. Tirri, “Transaction Management for M-commerce at a Mobile Terminal,” *Proc. of the 36th Annual Hawaii Int Conf on System Sciences*, IEEE 2003, pp. 89-98.

[6] E. Turban and D. King, *Introduction to E-Commerce*, Pearson Education, 2003, p. p. 336-337.

[7] D. Xioajun, I. Junichi and H. Shu, “Unique features of Mobile Commerce,” [cited 30/06/08]; http://www.is.me.titech.ac.jp/paper/2004/other/ebiz_ding.pdf. 2004, pp. 1-7.

[8] Y.H. Choi, S. Yoon, G. Shin and C. Park, “An Approach to Design of Software Architecture for Mobile-Commerce System,” *7th. Int Conf on Advanced Communication Technology*, IEEE 2005, pp. 924-926.

[9] W.-C. Hu, C.-W. Lee and J.-H. Yeh, “Mobile Commerce Systems,” *Mobile Commerce Applications*, Series Mobile Commerce Systems, ed., N. Shi, eds., Idea Group Inc. (IGI), 2004, pp. 2-23.

[10] U. Varshney and R. Vetter, “A Framework for the Emerging Mobile Commerce Applications,” *Proc. of the 34th. Hawaii Int Conf on System Sciences*, IEEE, 2001, pp. 1-9.

[11] A. Sergio, “M-commerce- What is it? What will it mean for consumers?,” [cited 15/06/08]; http://www.consumer.vic.gov.au/CA256902000FE154/Lookup/CAV_Publications_Reports_and_Guidelines/$file/mcommerce.pdf. 2002, pp. 1-13.

[12] R.A. Boadi and A.G. Shaik, “M-Commerce Breakthrough in Developing Countries: the Role of M-Commerce in Wealth Creation and Economic Growth in Developing Countries,” MSc dissertation, Dept. of Business Administration and Social Sciences, Lulea University of Technology, Sweden. 2006, pp. 1-92.

[13] A. Tsalgatidou and E. Pitoura, “Business Models and Transactions in Mobile Electronic Commerce: Requirements and Properties,” *Computer Networks, vol. 37, no. 2*, Elsevier Science B.V, 2001, pp. 221-236.

[14] G. Elliot and N. Phillips, eds., Mobile Commerce and Wireless Computing Systems, Pearson, 2004, pp. 415-417.

[15] S.J. Barnes, “Under the Skin: Short-range Embedded Wireless Technology,” *Int Journal of Information Management*, vol. 22, no. 3, Elsevier Science Ltd., 2002, pp. 165-179.

[16] R. Tiwari, S. Buse and C. Herstatt, “The Mobile Commerce Technologies: Generations, Standards and Protocols,” [cited 20/06/08]; http://www1.uni-hamburg.de/mcommerce/articles/Working_Paper_40.pdf. 2006, pp. 1-21.

[17] F. Perich, A. Joshi, Y. Yesha and T. Finin, “Neighborhood-Consistent Transaction Management for Pervasive Computing Environment,” *Proc. 14th Int Conf on Database and Expert Systems Applications* Springer, 2003, pp. 276-286.

[18] V. Patil and R.K. Shyamasundar, “Trust Management for E-Transactions,” *Sadhana,* vol. 30, no. 2 & 3, Indian Academy of Science, 2005, pp. 141-158.

Husna Osman received a Bachelor of Science degree in Computer Science from University of Science, Malaysia in 1995 and a Master of Science degree in Information Technology from University of Putra, Malaysia in 2001. She is currently a PhD student in the Department of Computer Science, Heriot-Watt University, Edinburgh, UK. Her research interests include wireless network security and ad hoc wireless networking.

Hamish Taylor (Dr) is a lecturer in the Department of Computer Science, Heriot-Watt University, Edinburgh, UK. His interests include peer to peer network applications, ad hoc wireless networking and virtual environments. He has also published in the areas of knowledge based systems, parallel databases and logic programming.

Appendix B

Published Paper: Managing Group Membership in Ad Hoc M-commerce Trading Systems

Managing Group Membership in Ad Hoc M-Commerce Trading Systems

Husna Osman and Hamish Taylor
Department of Computer Science,
Heriot-Watt University,
Edinburgh, Scotland. EH14 4AS.
ho12@hw.ac.uk and h.taylor@hw.ac.uk

Abstract—**Managing group membership in an ad hoc m-commerce trading forum is a challenging task as peers may only have partial knowledge of the current membership due to frequent network disconnections, infrequent participation and delays in communication via intermediaries among them. The absence of a centralized network infrastructure adds more complexity to this problem. This paper presents a fully distributed and self-organizing approach to managing group membership in such a loose trading community. It is designed to suit the dynamic nature of ad hoc wireless networking and the social characteristics of ad hoc m-commerce.**

Keywords-self-organized group; wireless trading; ad-hoc community; peer-to-peer

I. INTRODUCTION

A basic concept in ad hoc m-commerce trading systems is the formation of a trading forum by two or more peers that are in the vicinity of each other and run an appropriate software application. This trading forum defines the rules of trading and provides the context for mobile users to engage in mobile commerce using ad hoc wireless networking [1]. It is a self-organized and self-configured m-commerce domain that can be initiated by any peer with suitable networking capability and does not require any centralized infrastructure to manage it. Its participants communicate and cooperate with each other by utilizing their local resources and also their neighbours' to accomplish the following tasks:-

1) Engage in ad hoc m-commerce transactions such as swapping of digital resources, buying or selling items, mobile auctions, consortium trading and so on [1].
2) Give recommendations about other members' identities, trading histories and reputations.
3) Attest other members' digital certificates that bind together their identity information with their public keys.
4) Evaluate each other by providing deal evaluations of transactions.
5) Share negative evaluations about their trading partners with other members in the forum.
6) Sanction those members who misbehave or have a history of being given poor evaluations of their trades.

As an example, a group of peers with wireless networking capability and a mobile auction application installed on each device comes into communication range with each other. One of the peers reestablishes a trading forum that offers auction services and advertises it for other peers with similar interests to join. Peers able to join the trading forum session can then participate in the auction activities as sellers or bidders. The mobile auction application that runs on each peer's device handles all the auction processes and provides a graphical interface to the users. After the completion of each transaction, peers can provide deal evaluations to each other. Positive evaluations will increase a peer's reputation and thus increase other peers' trust and willingness to trade with that party in future transactions, while negative evaluations reduce other peers' confidence to transact with the peer and open that peer to the risk of sanctions from its trading forum.

One of the major security concerns in such trading systems is to establish sufficient trust among participating parties in a trading forum in order to mitigate the uncertainty and risks involved in its transactions. While some trading forums will choose to remain open to all comers, others will choose to use membership as a means for establishing greater trust and more secure interactions among its group members. As new parties may apply to join and existing members may have to be excluded, the management and maintenance of such trading forums entails support for a service to handle group membership.

The function of a group membership service is to track membership changes in a trading forum and help determine whether a peer is currently a member of a particular trading forum [2]. It consists of mechanisms for peers to join and be excluded from the trading forum, as well as to verify membership. However, to manage group membership in such a loose ad hoc m-commerce community with frequent and unpredictable network disconnections, infrequent communication among group members and in the absence of a centralized network infrastructure is a challenging

task as each member cannot be expected to have a complete or mutually compatible view of group membership.

Hence, this paper proposes a fully distributed and self-organizing approach for managing group membership in ad hoc m-commerce trading forums, which is based on membership vouchers, quorate decisions by some group members, partial membership lists and the use of digital signatures.

The rest of this paper is organized as follows. Section II describes solution requirements and assumptions. Section III gives a brief overview of related work. Section IV presents the details of each mechanism in our approach. Section V demonstrates a number of reference scenarios and finally, Section VI concludes the paper.

II. REQUIREMENTS AND ASSUMPTIONS

Due to the challenges posed by the nature of ad hoc wireless networking and the social characteristics of ad hoc m-commerce [1], the following requirements for managing a trading forum's group membership will be needed on top of the usual requirements for interactive m-commerce software such as adequate quality of service and reliability in the wireless network, end-to-end security and so on:

1) Resource-limited

The processes and operating costs of group membership management should be affordable for resource-constrained devices.

2) Dynamic

Group membership management should be able to handle dynamic membership changes without having to reconstitute the group.

3) Absence of Authority

The responsibility for managing the group membership has to be devolved among members without recourse to trusted parties with delegated authority as the presence of no party can be guaranteed in any live trading context.

4) Robustness

Intermittent participation by members, unreliable means of communication and the absence of dependable enduring infrastructure services requires failure tolerance throughout support for system services.

5) Convenience

The management of group membership should not involve users in complicated and time consuming activities nor should making changes in membership status take very long periods.

We assume that support for group members' identity establishment and verification is provided by a security and trust service. Details and discussion of this are part of ongoing work and will be published later. We illustrate in Fig. 1 below an abstract architecture for each trading peer in an ad hoc m-commerce trading forum. The first two layers sequentially include a mobile device and an operating system required for operating the applications. The Service layer provides services that are required to support the core functionality of the trading system which include the following:

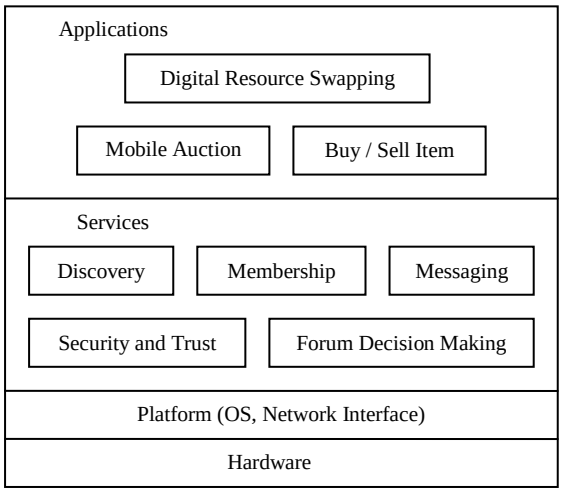


Figure 1. An abstract architecture for an ad hoc m-commerce trading peer.

- Discovery Service
  Provides the ability for peers to search and discover available trading forums, advertisements and other peers in the network

- Membership Service
  Provides the ability for peers to organize themselves into a trading forum, which includes the ability to join, renew membership and also to exclude a member from a trading forum.

- Forum Decision Making Service
  To facilitate any decision making processes by fostering effective communication among forum members.

- Messaging Service
  Provides support for message delivery over the network. This includes specifications for routing, relaying and propagating messages as well as the message structure and so on.

- Security and Trust Service
  Provides support for identity establishment, trust establishment as well as message authentication, integrity, confidentiality and non-repudiation. This service will also provide security advice to make participating users understand the issues and their responsibilities in securing ad hoc m-commerce trading systems.

The Application layer is the implementation of ad hoc m-commerce applications such as mobile auctions, swapping of digital resources, buying or selling items and so on.

III. RELATED WORK

Several relevant papers have been published in the area of group membership in ad hoc wireless

networks such as [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]. The main focus of most of the work is to provide secure communications among group members, in which some of the solutions proposed are based on group key agreements. Maki, Aura and Hietalahi in [5] have proposed a distributed certificate-based system to establish secure communications among members in ad hoc groups, where a certificate that is signed by a group key is used to indicate the membership of each member. The group key is used as the identifier of the group and is generated by a group leader who is responsible for managing the group membership. To avoid a single point of failure, a group leader's authority is distributed to multiple sub-leaders. Thus, a group can have one or more group leaders or sub-leaders. A similar approach is used by Steiner, Tsudik and Waidner in [6] to address the issue of secure group communications in dynamic peer groups. They have proposed a protocol called CLIQUES which is based on a multiparty extension of Diffie-Hellman key exchange. In this protocol, all members contribute to the establishment of a group key. Whenever there is a membership change, the group key is reconstructed. This approach also depends on having a group controller to manage the group membership. Liu, Sacchetti, Sailhan and Issarny [13] in their design of a generic group management service for mobile ad hoc networks (MANET) have also proposed a group leader for managing the group dynamics. In their approach, the group leader's role is rotated from one member to another in order to distribute the load of group management among members and also to address the issue of group leaders dropping out of participation. The selection of the group leader is based on a number of criteria that have been defined [13].

Another approach is a virtual partitioning (VP) based group membership algorithm by Pradan and Helal [10]. This approach requires each group member to maintain a complete and consistent view of group membership. Roman, Huang and Hazemi in [4] have also proposed an algorithm to maintain a consistent view of group membership in ad hoc wireless networks based on location information.

Group key agreement does not seem to be workable for ad hoc m-commerce trading forums. Participation by all members on a regular and frequent basis would be required in order that new group keys could be constructed in a timely way for each membership change and also for each member to get access to the new group keys every time they are reconstructed. However, casual local online trading is likely to involve a mixture of frequent and infrequent participants and quite an amount of irregular participation. Thus, it may not be possible for a new group key to be constructed in a timely way for each membership change on each occasion that requires contribution by all group members. It will take unpredictable periods of time for all members to be available for the reconstruction process to happen. This might delay the first opportunity for a new member to participate in the group communications as well as other activities of the trading forum. This might also give an opportunity for a member subject to exclusion proceedings to remain as a member for a longer period of time. On other occasions, the unavailability of some members during the reconstruction of the group key might cause them to be unable to get access to the new group key and thus might lead to the group shrinking as a subset of the members reconstruct the group key among themselves. The reacceptance of these unavailable members in the trading forum would demand the group key be reconstructed again. This might lead to endless reconstruction of group keys as frequent and regular participation by all group members cannot be guaranteed in ad hoc m-commerce trading forums.

A hierarchical structure where one or more group leaders are responsible for managing the group membership also does not seem to be workable for our work as the presence of such authority in the current group context cannot be guaranteed all the time. Furthermore, the loose nature of relationships in casual local trading networks does not support the assumption of a core of well trusted parties around which the rest of the trading community is constituted. Thus, a flat structure where all members are given equal responsibility to manage the group membership would seem to be more appropriate.

The requirement for each member to maintain a complete and consistent view of current group membership is also not realistic for ad hoc m-commerce trading forums. Communication among members will often involve intermediaries, be subject to frequent disconnections and take unpredictable periods of time from minutes to several days or weeks with infrequent participants. Getting all group members to participate in every membership decision will take too long to be practical. So membership decision making needs to be delegated to subsets of the membership and other members will have to accept their decision making when it is eventually communicated to them. That in turn means that every member will only have a partial view of the membership.

IV. APPROACH

In this section, we describe our approach for managing group membership in ad hoc m-commerce trading forums.

A. Membership Voucher

A membership voucher serves as a credential that can be used by forum members to prove their membership to other members of the forum. It contains the following information as a minimum:-

- The trading forum name and ID.
- Its holder's trading pseudonym or ID.
- The collection of approvals and any vetoes among verified votes. Each vote will consists of the voter's trading pseudonym

or ID, the subject of the vote either a joining request or membership renewal request, the requestor's trading pseudonym or ID, voter's agree or disagree statement, time and date as well as the digital signature of the voter.

- Digital signature of its issuer.
- A validity period.

To be recognised as a member of a trading forum, each peer must possess a membership voucher that is digitally signed by other group members who are expected to be recognised. A recognised member is a member whose membership voucher has been verified as having the following:-

- Its validity period has not expired.
- Has been issued and signed by parties who are recognised as members at the time the membership voucher is issued.
- Has sufficient number of votes from parties who are recognised as members at the time they participated in the vote.

Peers present the voucher and their certificate to attest their membership and receiving peers use the resources available to them such as personal records of previously known members of the forum to decide whether to accept the claim. Members exchange these records with other trusted members to widen and update their views of the scope of membership. However, as the judgments are made independently by each peer based on their partial membership views without involving any authority higher than a peer, membership claims cannot always be settled to the satisfaction of all reasonable peers. It will depend on the level of trust that the receiving peers have in the issuer and the voters of the presenting peers' membership voucher as well as the parties that attest their membership vouchers. If the receiving peers trust those parties, it is expected that they will accept the presenting peer's membership claim.

The validity period of the voucher is used as a regular way to review the membership status of each member. After its expiry date has elapsed, the voucher is no longer applicable to prove a peer's membership. Thus, to remain as a current member of a particular trading forum, each peer needs periodically to renew their membership voucher when the existing voucher expires.

B. Quorate Decisions

As members of a trading forum are peers that have similar constraints on their devices and are offline most of the time, it is not realistic to expect to have a trusted peer or unbroken chain of trusted peers to be responsible for managing the group membership that is reachable all the time. All peers are given equal responsibility in order to avoid circumstances where decisions cannot be made due to the unavailability of an appropriate authority. Therefore, in this work, the decisions to accept new members, exclude misbehaving members and also renew existing members' membership vouchers are distributed to any sufficiently large subset of existing group members. How many members need to agree and the maximum number of members allowed to disagree in order to elicit a quorate decision will depend on each trading forum's decision making policies.

A trading forum's decision making policy can be made simpler or more stringent depending on the type of ad hoc m-commerce trading. A simple policy is probably more desirable for circumstances that entail fast decision making, such as in the admission process. It may require only a small number of approval replies and no vetoes. For example, a trading forum with 30 current members may require only a small fraction of currently active and connected members to agree and none to disagree, in order to obtain a quorate decision whether to accept or reject the application of a new member. By having such a policy, new admissions could take place rapidly. On the other hand, to obtain a quorate decision for a more stringent decision making policy might require a definite higher number of approvals and less than a threshold number of vetoes. This may involve currently offline members as the replies from currently connected members may not be sufficient to obtain a quorate decision. However, to elicit the required number of members' votes may take some time as many members may not be reachable for significant periods or may not participate frequently in group communications. Thus, this type of policy might be more appropriate for circumstances that do not require rapid decision making such as in the membership renewal process or exclusion of members, which require more careful consideration. For example, to exclude a member from a trading forum of 40 current members might require at least 20 members to agree and less than 5 members disagree with the exclusion proposal.

C. Membership Lists

A membership list contains records about sometime members of a trading forum. It also provides information about the status of each member as to whether a member is a current member or former member or has been excluded. A complete membership list would keep members updated with the current membership of a particular group [10].

However, all members of an ad hoc m-commerce trading forum cannot be expected to have a complete and consistent view of membership as some of them may be offline or unreachable or may not participate in group communications regularly or may be active but not yet have had messages passed on to them about decisions taken by other members. Instead, members of an ad hoc m-commerce trading forum will each maintain a partial list of members and exclusions that they know about and accept in their local storage and exchange it with other members

to update and widen their view of membership every time they participate in the trading forum.

D. Digital Signature

A digital signature is used to guarantee the authenticity and integrity of a message or document sent by a peer as well as to ensure that the sender cannot get away with denying having sent the message or document. In ad hoc m-commerce trading forums, messages and documents such as membership requests, votes, membership vouchers, exclusion proposals and also exclusion orders are digitally signed by their sender in order to give assurance to the receiving peers that those messages or documents were actually sent by the specified sender and were not altered during transmission and also so that the sender will not be able to credibly deny having sent the message.

E. Join Mechanism

For a new member to join a trading forum, he must first discover a member of the forum and then send a join request. The following steps are involved:-

1) Sending a request to join

A new member (M_{new}) sends a join request message together with his digital certificate to at least one member of the trading forum. The certificate must be self-signed but may also be signed by other parties. The join request message will contain the following information as a minimum:-

- The target trading forum name and ID
- M_{new}'s trading pseudonym or ID
- Digital signature of M_{new}

2) Propagate Join Request

Upon receiving the join request message, the contacted member ($M_{contact}$) will then propagate it to other members of the forum in order to obtain a quorate decision whether to accept or reject the application. The propagated message will have a time limit (TTL) in order to limit the voting period. However, $M_{contact}$ may consider having extra rounds of voting if the verified votes received are not sufficient to obtain a quorate decision after the voting period limit has expired.

3) Quorate decision by other members

Other members of the forum with views on the proposal are then expected to reply with either a signed agree or disagree message to $M_{contact}$, accompanied by their membership voucher as a proof of their membership.

4) Issuance of membership voucher

Upon receiving the replies, $M_{contact}$ will verify the voters' membership vouchers as not having expired and as being of members $M_{contact}$ recognises as members or having sufficient signatures of parties $M_{contact}$ recognises as members at the time the membership vouchers were issued. Fig. 2 below depicts the steps involved in the verification process. Votes that are not verified or are received after the time limit are discarded. Then the forum's admissions policy is applied to the verified votes. If there are sufficient acceptances and less than sufficient vetoes, $M_{contact}$ will send a signed standard membership voucher to M_{new}. In addition to a membership voucher, $M_{contact}$ will also send his local partial lists of known members and known members to be excluded to M_{new}.

5) Update membership list

M_{new} will then notify other members about his new membership by multicasting a Hello message accompanied by his membership voucher to all currently active and connected members of the group. They will pass the multicast on during further group interactions until the multicast message's liveness expires.

Upon receiving the votes, $M_{contact}$ will execute the following algorithm:-

```
Check whether the validity period of the voter's membership voucher is still applicable
If yes
  Check whether the voter is a recognised member in his membership lists
  If yes
    Accept vote
  Else
    Check whether the voter's membership voucher is issued and signed by a recognised member at the time it is issued and has sufficient votes from recognised members at the time they participated in the vote
    If yes
      Accept vote
    Else
      Check whether the membership voucher of the unrecognised issuer and voters are issued and signed by a recognised member at the time it is issued and has sufficient votes from recognised members at the time they participated in the vote
      If yes
        Accept vote
      Else
        Discard vote
Else
    Discard Vote
```

Figure 2. Voter's membership voucher verification steps.

F. Exclusion Mechanism

To induce participating parties in ad hoc m-commerce trading systems to act honestly and in a trustworthy way, it is valuable to have a mechanism to sanction forum members that misbehave or have a history of being given poor evaluations of their trades. One of the appropriate ways to do this is exclusion from membership. By having a mechanism to exclude misbehaving members, a group membership service can provide a degree of assurance about forum members' trustworthiness and reputations. It will sit alongside the reputation system, which is one of the elements in our security and trust service, and serves as the primary service to help assess the behavior and also the trustworthiness of each member.

Similar to the join process, to exclude an existing member requires a quorate decision from other members of the trading forum. The following steps involved:-

1) Multicasting a proposal to exclude

An existing member ($M_{propose}$) can propose to exclude a misbehaving member or a member with poor evaluations from a trading forum by multicasting a proposal to exclude message to other forum members except the target member (M_{target}). The message will consist of the following information:-

- The target member's ID or trading pseudonym.
- $M_{propose}$ digital signature

In addition to that, an accompanying note giving brief reasons for the exclusion might also be expected.

2) Quorate decision by other members

If other forum members agree or disagree with the exclusion proposal, they will reply with a signed agree or disagree message to $M_{propose}$ within the required time period. The message will consist of similar contents as in the votes for joining and membership renewal request as mentioned in section IV (A) above, except that the message subject will be the exclusion proposal. In addition to that, the trading pseudonym or ID of the proposed member to be excluded will also be included in the message.

3) Multicasting an exclusion order

Once enough replies from validated members are collected within the voting time period limit and the forum's exclusion criteria are satisfied, $M_{propose}$ will then multicast an exclusion order to other currently connected members. The exclusion order will have the following details:-

- The target's trading pseudonym or ID
- The collection of signed messages approving and disapproving the target's exclusion.
- Digital signature of $M_{propose.}$
- Exclusion period

In this case, forum members are expected to refrain from issuing a new membership voucher to the target member after the validity period of his current membership voucher has expired until the exclusion period has ended. Also, any votes or membership vouchers issued by the target member will not be considered as valid. Furthermore, forum members are also expected to not participate in any transactions with that member.

G. Membership Renewal Mechanism

To remain as a member of a trading forum, each member should renew their membership near the end or after the validity period of their current membership voucher expires. The following steps are involved:-

1) Sending a membership renewal request

A member who holds an expired or soon to expire membership voucher sends a membership renewal request together with his old or current membership voucher to at least one of the current members of the trading forum ($M_{contact}$).

2) Propagate Renewal Request

Similar to the join and exclusion mechanisms, to renew a membership voucher also requires a quorate decision from other forum members. Thus, upon receiving the membership renewal request, $M_{contact}$ will then propagate it to other forum members in order to obtain a quorate decision whether to accept or reject the renewal request.

3) Quorate decision by other members

In this situation, other members are expected to check whether any non-expired order has been issued to exclude the requesting member from the trading forum before they each reply with either a digitally signed agree or disagree message together with their valid membership voucher to $M_{contact}$.

4)Collate agree messages

Once enough replies from validated members are collected within the voting period limit and the forum's membership renewal criteria are satisfied, $M_{contact}$ then collates the replies and sends them together with a new membership voucher to the requesting member. The voucher is signed by $M_{contact}$ as an accurate record of the vote.

H. Message Propagation

In this work, each message is associated with a unique identifier and a time to live (TTL). To ensure reliable message propagation, each time a peer receives a message for the first time, it will accept the message, store it and also forward it once to each of its directly connected neighbours except the sender during the period of its lifetime. To prevent duplicate propagation, each time a peer receives the same message more than once, the message will be discarded. As all of the mechanisms discussed above require sufficient members' votes to obtain a quorate decision, it is important for each voting activity to have an expiry time. Therefore, the use of a TTL will ensure that each propagated message is discarded after its time limit has expired.

V. REFERENCE SCENARIOS

We demonstrate each of the above mechanisms in a series of scenarios below.

A. Scenario 1 – Joining

A trading forum A consists of 5 members M_1, M_2, M_3, M_4 and M_5. All members are online during communication period t_1. It is assumed that:-

- Each of them possesses a current membership voucher
- Each member's local membership list contains the membership records of other members as follows:
  M_1 (M_2, M_3, M_4, M_5)
  M_2 (M_1, M_3, M_4, M_5)
  M_3 (M_1, M_2, M_4, M_5)
  M_4 (M_1, M_2, M_3, M_5)

M_5 (M_1, M_2, M_3, M_4)

- No member has any knowledge of parties to be excluded.
- This trading forum applies a simple admissions policy that requires at least three members agree with the new application and none disagrees while votes are being gathered.

A new member M_6 comes into their communication range and sends a join request to M_2 together with his self-signed digital certificate. M_2 then propagates the request to other members. It is assumed that all members agree to accept the new application from M_6. They then each reply to M_2 with their digitally signed agree message together with their membership voucher. Upon receiving the replies, M_2 will then verify each of the voters' membership vouchers. In this case, all votes are accepted as each of the voters possesses a current membership voucher and M_2 recognises them all as members in his membership lists. M_2 then applies the trading forum's admissions policy to the verified votes and sends a signed standard membership voucher containing the four signed approvals and its local membership list to M_6. M_6 then sends a hello message together with his membership voucher to other connected members in order to notify them of his new membership. Upon receiving M_6's hello message and membership voucher, other connected members will independently verify M_6's membership voucher before accepting the new membership and update their local membership list. This scenario is illustrated in Fig. 3 below. At the end of communication period t_1, the local membership list of each member will be as follows:-

M_1 (M_2, M_3, M_4, M_5, M_6)
M_2 (M_1, M_3, M_4, M_5, M_6)
M_3 (M_1, M_2, M_4, M_5, M_6)
M_4 (M_1, M_2, M_3, M_5, M_6)
M_5 (M_1, M_2, M_3, M_4, M_6)
M_6 (M_1, M_2, M_3, M_4, M_5)

B. Scenario 2 – Exclusion

This scenario takes place after the earlier one. It is assumed that:

- During this communication period, trading forum A consists of 20 parties (M_1, M_2, ……, M_{19} and M_{20}) that possess a current membership voucher. However, only M_1, M_2, M_3, M_4, M_8, M_{10}, M_{15}, M_{16}, M_{17} and M_{19} are online while the others have gone offline.
- This trading forum applies an exclusion policy that requires at least 7 members to agree with the exclusion and less than 3 vetoes before any member can be excluded.
- The local membership list of each currently connected member contains the membership record of other connected members as each of them needs to send a hello message together with their membership voucher to all connected members in order to rejoin the trading forum after being offline or disconnected from the network.

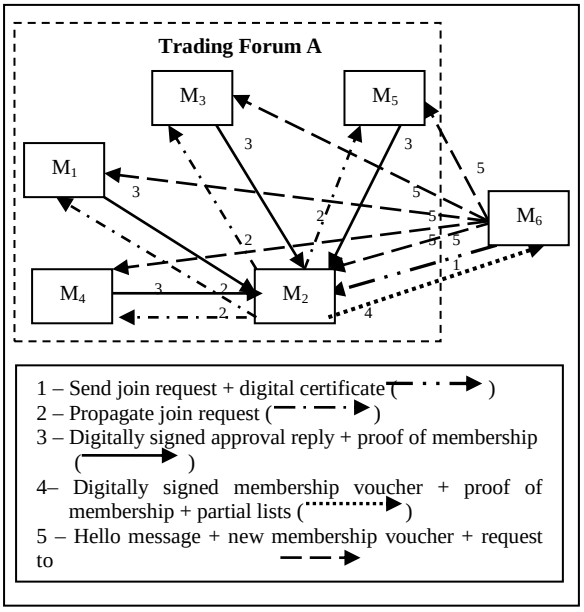


Figure 3. A join scenario with five members (all online).

M_2 multicasts a proposal to exclude M_8 to all currently connected members of the forum except M_8. It is assumed that all reply and only M_1, M_3, M_4, M_{10}, M_{15} and M_{19} agree with the exclusion proposal while the others disagree, and M_2 receives their digitally signed votes within the voting period limit. Upon receiving the votes, M_2 then verifies the voters' membership voucher and accepts their votes as the validity period on their membership vouchers are still applicable and M_2 recognises them all as members in his local membership list. After adding his own approval vote and the forum's exclusion policy is applied, there are sufficient number of approvals (7 approvals) and less than sufficient vetoes (2 vetoes) for M_2 to obtain a quorate decision to issue an exclusion order. M_2 then multicasts the exclusion order to all connected members except M_8. This scenario is illustrated in Fig. 4 below.

C. Scenario 3 - Renewal

In this scenario, trading forum A consists of 25 current members (M_1, M_2, ….M_7, M_9, ……, M_{25}) and it is assumed that:

- In the beginning, only M_1, M_4, M_6, M_7, M_9 and M_{10} are online while the others are offline.
- M_1's membership voucher is nearly expired.
- Renewal policy requires at least 7 members to agree with the renewal request and no vetoes before any new membership voucher can be issued to the requesting member.

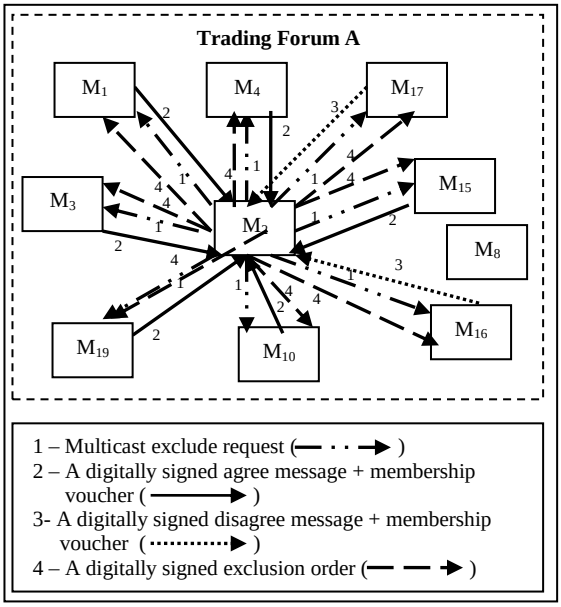


Figure 4. An exclusion scenario

M_1 sends a membership renewal request together with his current membership voucher to M_9 who then propagates the request to other currently connected members. It is assumed that only M_4, M_6 and M_7 agree with the request and reply with a digitally signed agree message together with their membership voucher to M_9 as depicted in Fig. 5 below. It is assumed that M_{10} received the propagated message but decided not to participate in the vote. Upon receiving the agree replies, M_9 then verifies M_4, M_6 and M_7s' membership vouchers and accepts their votes as the validity period on their membership voucher is still applicable and M_9 recognises them as members in his local membership list. However, in this situation, the number of approval replies is still not sufficient for M_9 to obtain a quorate decision to issue a new membership voucher to M_1. Thus, M_9 has to wait until the voting period limit expires before he can consider a second round of voting.

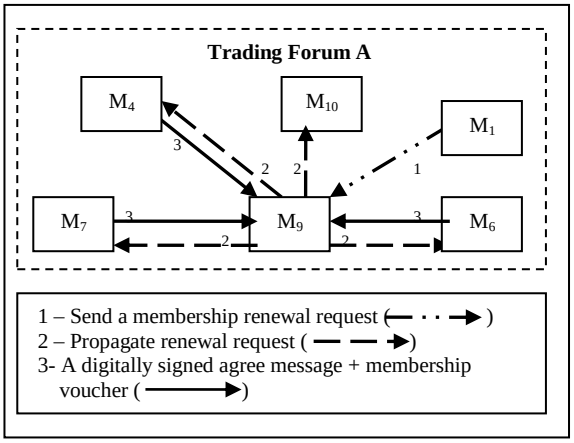


Figure 5. A renewal scenario

After some further time has elapsed within the same voting period limit, it is assumed that M_4, M_6, M_7 and M_{10} have gone offline while M_2, M_5, M_{20}, M_{23}, and M_{25} come into communication range with M_1 and M_9. The others remain offline. M_9 then propagates the membership renewal request to M_2, M_5, M_{20}, and M_{23} after receiving their Hello Message and verifies their membership voucher. In this case, it is assumed that M_9 did not accept M_{25}'s membership claim as he did not recognise either the issuer of M_{25}'s membership voucher or the issuer and voters of that issuer as members in his membership list. Thus, the renewal request is not propagated to M_{25}. M_2, M_5, M_{20}, and M_{23} agree with the request and they each reply with a digitally signed agree message together with their membership voucher to M_9 within the voting period limit. M_9 then validates their votes. Validated votes from M_2, M_5, M_{20}, and M_{23} as shown in Fig. 6 below now enable M_9 to obtain a quorate decision to issue a new membership voucher to M_1.

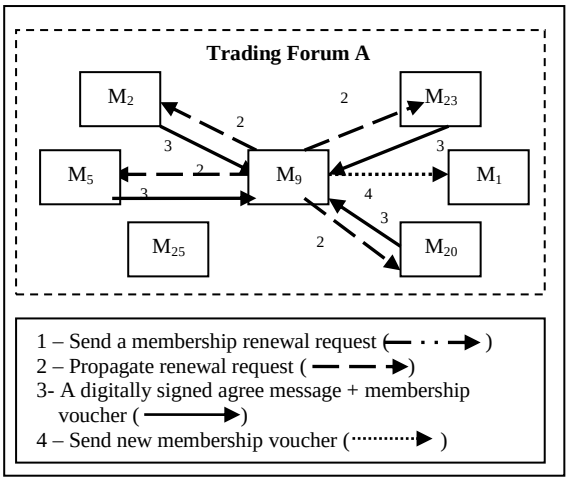


Figure 6. Issuance of a new membership voucher.

VI. CONCLUSION

In this paper, we have argued for the value of having a group membership service in ad hoc m-commerce trading forums in order to establish greater trust and more secure interactions among its group members.

Our approach does not rely on a complete knowledge of the current group membership to determine whether a peer is a member of a particular trading forum. Furthermore, it does not demand all group members to participate in group communications frequently and regularly in order for a quorate decision for group membership management to be able to be obtained. However, as the attestation process does not involve any authority higher than a peer and is done independently by each peer based on their partial knowledge of group membership, membership claims acceptable to a sufficient number of peers to qualify may not be found acceptable by every other reasonable peer.

With this work, we aim to improve the security of ad hoc m-commerce trading systems by restricting participation to parties regarded as trustworthy by their peers. Our future work will be to implement and validate the proposed mechanisms with some experimental results.

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their valuable and helpful comments in improving this paper.

REFERENCES

[1] H. Osman and H. Taylor, "Towards a reference model for m-commerce over ad hoc wireless networks," *Proc. E-Activity and Leading Technologies (E-ALT) Conference*, 2008, pp. 223-232.

[2] K.S. Barber, R. McKay and T-H. Liu, "Group membership services for dynamically organized sensible agent-based systems," *Proc. 12th. International FLAIRS Conference*, AAAI, 1999, pp. 160-165.

[3] A. Ricciardi and K. P. Birman, "Process membership in asynchronous environment," Technical Report TR 93-1328, Department of Computer Science, Cornell University, 1993, pp. 1-42.

[4] G. Roman, Q. Huang and A. Hazemi,"On maintaining group membership data in ad hoc networks," Technical Report WUCS-00-26, Washington University, 2000, pp. 1-11.

[5] S. Maki, T. Aura and M. Hietalahti, "Robust membership management for ad-hoc groups," *Proc. 5th Nordic Workshop on Secure IT Systems)*, 2000.

[6] M. Steiner, G. Tsudik and M. Waidner, "Key agreement in dynamic peer groups," IEEE Transactions on Parallel and Distributed Computing, vol. 11, no. 8, IEEE, 2000, pp. 769-780.

[7] P. Adusumilli, X. Zou and B. Ramamurthy., "DGKD: Distributed group key distribution with authentication capability," *Proc. IEEE Workshop on Information Assurance and Security*, IEEE, 2005, pp. 286-293.

[8] A. Sjoholm, L. Seitz and B. Sadighi, "Secure communication for ad-hoc, federated groups," *Proc. 7th Symposium on Identity and Trust on the Internet*, ACM, 2008, pp. 48-58.

[9] M. K. Sbai, E. Salhi and C. Barakat, "A membership management protocol for peer-to-peer services in MANET," INRIA-00342691, version 2, 2009, pp. 1-9.

[10] P. Pradan and A. Helal, "An efficient algorithm for maintaining consistent group membership in ad hoc networks," *Proc. 23rd International Conference on Distributed Computing Systems*, IEEE Computer Society, 2003, pp. 428-433.

[11] K.-Y. Rhee, Y.-H. Park and G. Tsudik, "A group key management architecture for mobile ad-hoc wireless networks," Journal of Information Science and Engineering, vol. 21, 2005, pp. 415-428.

[12] M. Filali, V. Issarny, P. Mauran, G. Padiou and P. Queinnec, " Maximal group membership in ad hoc network," in Lecture Notes in Computer Science, Springer Berlin, 2006, pp. 51-58.

[13] J. Liu, D. Sacchetti, F. Sailhan and V. Issarny, "Group management for mobile ad hoc networks: design, implementation and experiment," *Proc. 6th. International Conference on Mobile Data Management*, ACM, 2005, pp. 192-199.

[14] D. Bottazi, R. Montanari and G. Rossi, "*A self-organizing group management middleware for mobile ad-hoc networks*," Computer Communications, vol. 31, no. 13, Elsevier, 2008, pp. 3040-3048.

[15] L. Briesemeister and G. Hommel, "Localized group membership service for ad hoc networks," *Proc. International Conference on Parallel Processing Workshops*, IEEE Computer Society, 2002, pp. 94-100.

[16] L. Galluccio, G. Morabito and S. Palazzo, "Spontaneous group management in mobile ad hoc networks," Wireless Networks, vol. 10, no. 4, Kluwer Academic Publishers, 2004, pp. 423-438.

Appendix C

Published Paper: Identity Support Scheme in a Security and Trust Service for Ad Hoc M-commerce Trading Systems

Identity Support in a Security and Trust Service for Ad Hoc M-Commerce Trading Systems

Husna Osman and Hamish Taylor
Department of Computer Science,
Heriot-Watt University,
Edinburgh, Scotland. EH14 4AS.
ho12@hw.ac.uk and h.taylor@hw.ac.uk

***Abstract* – Ad hoc m-commerce is an emerging way of conducting online trading wirelessly within dynamic network communities. However, participants in such systems are vulnerable to attacks on identity establishment such as spoofing and whitewashing as part of fraudulent and unfair trading practices. This paper presents a scheme for identity support using PGP certificates in a fully self-organised manner, where a trading pseudonym and photograph are used as identity credentials. It lets participating parties collaborate in a Peer-to-Peer (P2P) way to establish their online identity in a manner that is resistant to such attacks without any mediation of a Certification Authority (CA). It also lets participating parties handle the security settings of the trading system as well as share knowledge about fellow participants' trading behaviour without relying on support from a network service provider.**

Keywords – casual local trading, collaborative service, ad hoc community, infrastructure-less service, PGP

I. INTRODUCTION

An ad hoc m-commerce trading system is a type of casual local trading facility conducted online and wirelessly outside established computer networks. It enables mobile users to organise themselves into a trading forum regardless of time or location without relying on any infrastructure support from a network service provider [1]. Members of a trading forum will utilize available computing resources to communicate and participate in activities such as m-commerce transactions, membership management, attestation processes and so on. However, since such activities are carried out over ad hoc wireless networks and as no network service provider can be relied upon to provide security services, this type of trading system is vulnerable to various types of attacks that undermine its functionality and dependability. These include identity spoofing, Sybil attacks, man-in-the-middle attacks, unfair evaluations, collusions and misleading trade descriptions.

Public key cryptography provides a variety of techniques for online identification, which can be used to protect traders against attempts to misrepresent identity. Such identity support can be used as part of a security and trust service to protect the authenticity, integrity, confidentiality and non-repudiation of information being exchanged, as well as to establish a tight binding between a trader's identity and its reputation and membership information. The identity-reputation binding enables traders to assess the trustworthiness of other traders. The identity-membership information binding helps traders to determine the validity of each member's membership voucher and also each vote made by participating parties in collaborative decision making processes for membership management. In ad hoc m-commerce trading systems, a membership service could keep track of a trading forum's membership and help determine the current membership status of each participant. It would consist of mechanisms for traders to join, to verify other parties' membership and to exclude those that do not adhere to the trading forum's norms. Our scheme proposes that to be recognised as a member of a trading forum, a trader must possess a valid membership voucher that has a sufficient number of votes from recognised members of the forum, is digitally signed by a recognised member that issues it and its validity period must not have expired [2].

However, ad hoc m-commerce trading systems lack infrastructure services to support public key cryptographic mechanisms that rely on a trusted CA. They also cannot support self-organised substitutes that require one or more parties to be the certification authority for other peers as participation by those parties on a regular basis cannot be guaranteed in such a dynamic trading community. Identity establishment in ad hoc m-commerce trading systems requires a scheme that is peer to peer, independent of a pre-established network infrastructure and able to support infrequent communications among traders. This paper presents such a scheme for identity support for a security and trust service. It lets traders in an ad hoc m-commerce trading system establish their own online identity using Pretty Good Privacy (PGP) technology that uses a trading pseudonym and photograph as identity credentials in PGP certificates and supports a self-revocation mechanism. It also lets the traders collaborate in a P2P manner to handle the attestation process of those identities as well as to control other security elements of the trading system.

The rest of this paper is structured as follows. Section II discusses possible security threats and attacks on ad hoc m-commerce and their impact on trading systems. Section III describes the essential elements in security and trust services for such

systems. Section IV discusses the notion of online identity. Section V critically assesses related work. Section VI presents our approach for identity establishment in ad hoc m-commerce trading systems. Section VII concludes the paper.

II. POSSIBLE THREATS AND ATTACKS

There are several possible threats and attacks that can subvert the security of an ad hoc m-commerce trading system. We only focus on addressing the most common ones that significantly impact the functionality and dependability of such systems. We identify those threats and attacks and classify them into three categories:

A. Identity-related issues

Traders in ad hoc m-commerce trading systems are represented by their online identity, which we propose to handle with trading pseudonyms. Using pseudonyms to participate in online transactions in such a loose ad hoc community exposes them to the following security attacks.

1) Identity spoofing (masquerade)

Identity spoofing is where a party tries to pass himself off as someone else. The prime risk is that he may use that spoofed identity to defraud others.

2) Sybil Attacks

Sybil attack is where a party creates multiple identities to cheat collective decision making processes to subvert the trading system.

3) Whitewashing

A whitewasher is a party who leaves a particular forum and then re-enters with a new identity to hide his bad reputation.

B. Information-related issues

As exchanges of information in ad hoc m-commerce trading systems are conducted solely over insecure ad hoc wireless networks and may involve intermediaries, participants in such trading systems are vulnerable to man-in-the-middle attacks. Such an attack occurs when a party intercepts communications between two other parties and then tampers with or omits messages being transferred without the knowledge of either sender or recipient.

C. Misbehaviour-related issues

In ad hoc m-commerce trading systems, it is to be expected that traders will often engage in transactions with unfamiliar parties. This will make them susceptible to subversive behaviour by their trading counterparties such as:

1) Trade Misdescriptions

A party may cheat other traders by offering fake items as real or by trading items that are not as described in the offer.

2) Unfair Deal Evaluations

In ad hoc m-commerce trading systems, traders could be required to evaluate each other after the completion of each transaction by means of deal evaluations. They could be used to assess each trader's reputation and could consist of at least the following information.

a) The evaluator's trading pseudonym.

b) Transaction contract which is digitally signed by both parties and has a timestamp as a proof of a transaction.

c) Evaluation result that records the amount of satisfaction the evaluator receives from the trade.

d) The evaluator's digital signature.

If a transaction concludes positively, traders could be required to express their satisfaction in the deal evaluation, digitally sign it and then send it to their trading counterpart. Otherwise, they could share their bad evaluation with other traders in the trading forum. However, an ill-intentioned trader might manipulate the reputation of other traders by giving unfair deal evaluations. There are at least two types of unfair evaluations; overstatements and slanders. Overstatements give inaccurate positive evaluations to increase the reputation of a particular party while slanders attack the reputation of trading counterparties by giving inaccurate negative evaluations to lower their reputation.

3) Repudiation Misbehaviour

Repudiation misbehaviour occurs when a trader performs a particular action and then denies having performed it. There are at least two significant types of such misbehaviour; data and contract repudiations. Data repudiation occurs when a trader sends a message or document and then denies having sent it. Contract repudiation occurs when one party initiates a transaction or agrees on a transaction contract and then denies having initiated the transaction or having made the contract.

4) Collusions

Collusion is where multiple parties or a party with multiple identities conspire to influence their own or other traders' reputation, group decision making processes, attestation processes and so on.

The significant impact that these attacks have on the security of the trading systems is that they can undermine the reliability of the following:

a) The reputation service, e.g. a trader may conspire with associates to influence his own or other traders' reputations by providing unfair deal evaluations, which lead other traders into making incorrect trust decisions that result in unsatisfactory transactions.

b) Group membership management, e.g. multiple traders may collude to subvert collaborative decision making for group membership management or an intermediary may discard or alter a vote that is sent via his node without being detected by the end parties

c) Attestation processes, e.g. a trader may create multiple identities to provide bogus support for certificates.

d) Transaction activities, e.g. a trader may undertake a contract and then deny having made it.

III. SECURITY AND TRUST SERVICE

To create a sufficiently secure and trusted environment for traders to trade within ad hoc m-commerce trading systems, its security and trust service needs support for:

A. Identity

Identity support is probably the most crucial element in a security and trust service for an ad hoc m-commerce trading system. Robust means of identification will not only protect traders from attacks aimed at identity disguise, but also lets other elements of a security and trust service function properly and effectively. It provides a kind of security assurance for traders to communicate, collaborate, carry out transactions, manage membership and establish trust relationships with known other parties.

B. Message authenticity, integrity, confidentiality and non-repudiation

Support for message authenticity, integrity and non-repudiation is important to give assurance to participating parties that messages or documents being exchanged among them originated with their specified sender and were not altered in transit. Also, the recipients can be assured that the sender cannot credibly deny having sent them. Confidentiality will ensure that they are unreadable by eavesdroppers or intermediaries. Having these elements in the security and trust service will protect traders from man-in-the-middle attacks and repudiation misbehaviour.

C. Trust

The development of trust relationships among traders is vital to mitigate uncertainty and risks involved in the transactions. Parkhe in [4], describes uncertainty in online transactions as uncertainty about future transactions and about potential trading partners' behaviour in fulfilling their transaction agreements. These uncertainties create a perception of significant risk that might discourage traders from trading. A trust relationship established between two traders lets them believe that their counterpart is a sufficiently reliable and honest party to trade with and that the downside risks are low enough for them to expose themselves to. Thus, by having support for trust in the security and trust service, security issues related to potential misbehaviour can be mitigated.

D. Attestation

Attestation is significant as it provides a means for traders to vouch for other parties' credentials such as their digital certificates, membership status and reputation reports. It also helps to mitigate transaction risks, especially in situations that involve dealing with unfamiliar traders.

IV. THE NOTION OF ONLINE IDENTITY

In online trading, traders are represented by online identities. An online identity refers to a social identity that is established by users as a means to represent themselves in online communities. The main choice here seems to be between using their real identities such as their legal name, date of birth and home address or a trading pseudonym to represent themselves online. The use of a trading pseudonym would enable traders to participate in online trading incognito. It would also allow traders to keep their trading behaviour to a certain degree private. Furthermore, it would enable traders to project a distinctive trading persona that reinforces a reputation they wish to maintain. The real identity of a trader in terms of their legal name, date of birth and home address is not normally a relevant issue in online trading. The reputation of a trading pseudonym can be compromised just as easily as the reputation associated with a real identity. So the value of maintaining that reputation can act as a strong disincentive to abusing a trading pseudonym. By linking together reputation to a trader's pseudonym, the trustworthiness as well as future behaviour of that trader can be evaluated and predicted as long as a persistent identity is used. Pseudonyms make things harder where parties seek legal redress against criminal trading practices or contract violations. However, in casual local trading such recourses to law are rare and anyway the problem of converting a trading pseudonym to the real identity behind it needed in legal cases is not insuperable.

In ad hoc m-commerce trading systems, using real identities would create a problem of verification as no CA can be relied upon to have checked a trader's real identity credentials such as his identity card or passport to verify his identity. Attestors of such identities would have to assure themselves that a trader was entitled to call himself by his purported legal name, was actually born on the stipulated date and genuinely resided at the stated address which is hard for other traders to be sure of. However, in practice casual trading attestors want to attest an identity established by a recognised appearance and a recognised form of address for trading purposes. What the subjects are really called or when they were born or where they really live is beside the point. Also, using real identities can make it harder for traders to maintain secrecy about their engaging in particular transactions. Lack of secrecy can threaten a trader's privacy, put them at risk of harm from hostile competitors or even compromise the profitability of deals that they undertake. However, allowing pseudonyms raises the issue of whether it allows traders to create multiple identities or change their presented identity too easily. Traders might also try to hide their relation to a particular action like an attestation or vote and thus avoid being held accountable for that action. To prevent these issues in ad hoc m-commerce trading systems requires robust identification of traders. We propose doing this with digital certificates in a manner to be described in Section VI.

V. Related Work

A significant amount of research has been done in the area of public key management in ad hoc wireless networks and several solutions have been proposed in the literature [5-18]. This section will discuss briefly those which are relevant to our work. Rahman [11] has proposed using the PGP Trust Model to let users generate their own asymmetric key pairs as well as to function as independent CAs. Thus, any user in the network can sign and verify any other user's public key. These signatures progressively form a set of interconnected links of individual public keys or "Web of Trust" [9, 10]. The main interest in this approach is that it does not require a communal certification authority to vouch for a user's public key. However, Rahman's scheme requires a central key server to maintain a database of public keys which makes his approach unsuitable for ad hoc m-commerce trading systems as the responsibility for hosting the key server will be problematic in such a loose trading community. It will be difficult or impossible to resolve who would be responsible for providing and paying for the server and also whether all users would trust them to do that. Furthermore, uninterrupted connectivity with such a key server could not be guaranteed in such a network.

Capkun et al. [12] have proposed a fully self-organized approach to public key management that does not rely on any trusted authority or centralized infrastructure. It lets users generate their own public key pairs, issue digital certificates to others and authenticate each other by merging their local certificate repositories and then evaluate the authenticity of a public key based on the certificates available in the merged repository. Interesting aspects of this approach are that it enables users to distribute control of the security settings of the system and also to perform key authentication based on the available information in each user's local repository. It also does not require participation by all users during the authentication process. This approach seems to be suitable for our work due to its self-organised characteristic. However, its certificate renewal mechanism requires the same issuer to update a user's certificate and would not be appropriate in our work as regular participation by trading parties cannot be guaranteed. Traders with expired certificates would be at serious risk of having to wait for a long time to get in contact with their certificate issuer or never succeed if the issuer is no longer active or has been excluded from the trading forum.

Another fully self-organised approach has been described by Rachedi and Benslimane [13]. In their approach, they propose a distributed clustering algorithm to select a cluster head in each cluster, which is based on a trust value and mobility metric. The cluster head then becomes the CA in its cluster. The status of a CA node will change if other nodes do not receive any beacon from its node for a pre-defined period of time and a new CA will be elected. This approach does not seem to be workable either in ad hoc m-commerce trading systems as frequent changes in the CA role will make the attestation process unreliable. Furthermore, the role of a cluster head does not seem to be appropriate in a community of equals. Also, it cannot be expected that any prospective cluster head will be sufficiently trusted by all other traders in that cluster. While some parties will be trusted more than others by their fellow traders, many trading communities lack any prospect of achieving a consensus about which parties among them are worthy of enhanced trust.

VI. Our Approach

The motivation for our approach comes from acknowledging the self-organizing and infrastructure-less nature of ad hoc wireless networks and allowing participants in ad hoc m-commerce trading systems to control their security settings. Support for identity establishment will include generating public and private key pairs, generating, signing and verifying PGP certificates as well as revoking compromised certificates. The verification process will be done in a P2P manner without the intervention of a CA. All participants will play a similar role. We assume that:

a) Each trader maintains their own local certificate repository that contains their and other traders' certificates that they have attested or acquired.

b) Each trader creates their own trading pseudonym. To minimise the risk of more than one trader using the same pseudonym, traders are expected to check for this possibility against all trading pseudonyms that they have heard of.

c) Traders verify other traders' certificates based on their knowledge and recommendations from their trusted peers as detailed later in this section.

d) The trading software that is jointly used by traders to carry out transactions comes from a trustworthy source.

A. The creation of public/private key pairs

Using PGP technology [9, 10], each trader will create their own private-public key pairs locally.

B. The generation of digital certificates

Traders will also generate their own self-signed digital certificates locally. The format of the certificates will be in the form of PGP certificates. Each certificate will contain at least the following information:-

1) The certificate holder's public key.

2) The certificate holder's identity credentials. We propose using the holder's trading pseudonym and a photograph as their identity credentials. To do the verification, attestors can check the photograph against the appearance of party who asserts the enclosing certificate identifies them. One way to do the checking is by having a physical encounter which should be easy as traders trading via ad hoc

networking are likely to be in close proximity with each other. A photograph helps defend against Sybil attacks and whitewashing as traders cannot easily change their physical appearance and it will be detectable when multiple identities have similar photographic appearances.

3) The digital signature of the certificate owner.

4) The certificate's validity period. Each certificate will be issued with a standard limited validity period. Traders will have to generate a new self-signed certificate before the existing one expires and then send the newly generated certificate together with their current certificate to any forum members that they believe to be trustworthy for certificate verification. Certificates need to be time limited to some degree such as 5 years because aging changes physical appearance creating a mismatch with a photo.

5) The digital signature(s) of the certificate's attestor(s) and their certificate identifiers. Multiple recognised signatures on a single certificate give more assurance to the relying parties that the photograph and trading pseudonym in the certificate accurately identify a party with knowledge of the corresponding private key.

C. The verification of digital certificates

Since there is no inherent association between a public key and the identity credentials listed in the self-signed digital certificates, the validity of such certificates need to be attested by other parties to avoid an-ill intentioned trader from masquerading as others. In ad hoc m-commerce trading systems, as participating parties are peers who consider each other as equals, any peer can vouch for another peer's digital certificate. However, the validity of such a certificate will only be accepted if the relying party recognises a party who has vouched for the certificate as a trusted party. This process is based on the concept of a web-of-trust [9-11]. For example, if peer A trusts peer B sufficiently as an attestor, it is expected that peer A will accept the validity of peer C's digital certificate that is vouched by peer B. Anyone who trusts the attestor as an attestor, will consider any certificates signed by the attestor to be valid to the extent of that trust. To lessen the risk that any one certificate signatory is unknown or untrusted as an attestor, multiple signatories will usually be required.

D. Certificate Revocation

A certificate that has been compromised can only be revoked by its owner by performing the following steps:

1) First, generate a new private-public key pair.

2) Then, generate a new self-signed certificate that binds their identity credentials with the newly created public key. Traders are expected to use the same trading pseudonym for their identity credentials in order to maintain a persistent identity, so that their reputation can be retained.

3) Next, send the newly-generated certificate to members of the trading forum prepared to attest the validity of the certificate. Also they need to send their old certificate with it in order to use the same trading pseudonym.

4) Finally, multicast a revocation message that is signed by the new and old private keys together with the new and old certificates to other members of the forum. The receiving parties will update their local certificate repository by marking the old certificate as "compromised" and adding the new certificate to the list, if the signatures on the revocation message check out and their photos correspond. Otherwise the message and new certificate will be ignored.

To assure themselves that identity credentials in a PGP certificate really belong to the party that presents them, a trader can perform the following steps upon receiving a PGP certificate from unfamiliar traders. Some may require further checks depending on the outcome of the check or how careful the recipient is. Some may only be important if the currently proposed transaction has significant downside risks and the receiving parties want to be assured that the presenting party has a good trading history.

1) Check the trading pseudonym in the certificate against their store of certificates to see if a different certificate uses the same trading pseudonym. This step helps the recipient to discover attempts by an attacker to spoof the identity in that certificate. In this situation, the recipient should reject the presented identity as bogus if there is another certificate in his local certificate repository that use the same trading pseudonym yet has a photo of an obviously different person.

2) Check the self signature against the certificate's public key to ensure that the presenting party has not altered the contents of the certificate like the certificate's validity period or its owner's photograph. This step will protect against man-in-the-middle attacks.

3) Check the photo against the appearance of the subject when they are in a close proximity with each other. This step enables the recipient to check against an attempt by the subject to spoof another party's identity after discovering that party's private key.

4) Check the photo against their store of certificates to see if that appearance is used with a different identity. This enables the recipient to detect any attempt by the presenting party to be a whitewasher or to create multiple identities.

5) Check that a certificate with that public key is not recorded as 'compromised' in his local certificate repository. This will prevent the attacker from further abusing a spoofed identity. It could also be used as

evidence to exclude the presenter from a trading forum's membership for conducting himself inappropriately.

6) Check whether the certificates of any trusted third parties that have signed the presented certificate are available in his local certificate repository. They can provide reassurance that the presenting party with the given appearance is entitled to use the trading pseudonym. Any attempt by those third parties to attest a false identity of the presenting party could expose them to the risk of being excluded from a trading forum's membership. This provides a modicum of accountability for subversive behaviour.

7) Check that the photo appearance is not very similar to that of anyone that there have been broadcast warnings about or about whom an exclusion proposal has been issued. This will give some kind of assurance to the recipient that the certificate is not an alleged malefactor. It would also throw suspicion on the good faith of the signers of the presented certificate.

8) Check that the validity date on the certificate has not expired. An expired certificate doesn't disprove the identity of its presenter but it does raise doubts about the usefulness of the photo and about whether the presenter has had difficulties finding trustable third parties to sign a current certificate for that party.

To mitigate security issues related to misbehaviour of a trader, a distributed reputation system that employs a sanction-backed mechanism will be used as a means to facilitate trust development among traders [3]. An exclusion mechanism [2] that is based on collaborative decision making by a sufficiently large number of forum members is recommended for use to sanction traders that misbehave or have a poor reputation. This will be a strong incentive for traders to behave appropriately especially in fulfilling their transaction agreement and providing truthful deal evaluations and testimonials as they will be open to the risk of being excluded from a trading forum's membership if other traders receive complaint about their misbehaviour and also an exclusion proposal. A trader's public key and a transaction contract that is digitally signed by both parties involved in the transactions, which are included in the deal evaluations will establish a tight binding between a trading party's identity and its reputation.

VII. CONCLUSION

With this work, we introduce a novel form of support for ad hoc m-commerce that aims to create a sufficient degree of confidence among traders to participate in such a casual local wireless trading, as well as to serve as a basis for establishing an m-commerce domain in a totally self-organizing and P2P manner. In the design of a security and trust service for such trading systems, we have identified and discussed three main categories of threats and attacks that have significant affects on its security. We contend that by addressing these three main categories of threats and attacks, an environment that is sufficiently secure and trusted can be created for traders to communicate, collaborate and carry out transactions. We also contend that by providing robust identification support, such security threats and attacks can be prevented or at least mitigated.

We have also discussed the notion of online identity in the context of online trading. We propose a mechanism that allows participating parties of an ad hoc m-commerce trading system to establish their online identity in a fully self-organizing manner using a trading pseudonym and a photograph as their identity credentials in a PGP certificate. It also allows collaboration among those parties to control the attestation process of such PGP certificates without relying on any trusted certification authority. We discussed the steps that can be performed by a recipient of such a PGP certificate in our approach to resist security attacks against online identity. However, as the attestation process is done totally in a P2P manner among traders without involving any higher certification authority and is based on each attestor's knowledge, identity credentials presented in a PGP certificate that is acceptable to some parties may not be found acceptable to every other party in the trading forum. It will depend solely on the level of trust that the recipients have in the parties that attest the PGP certificate.

We intend that this work together with our proposed group membership service [2] and a reputation system [3] will be able to support security for an ad hoc m-commerce trading system to a sufficient degree for trade to be viable using it. A limitation of this approach is that no implementation has yet been attempted to evaluate its effectiveness. Our future work will attempt to validate our proposed security and trust service with some experimental results using real life scenarios and security expert reviews.

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their valuable comments in improving this paper.

REFERENCES

[1] H. Osman and H. Taylor, "Towards a reference model for m-commerce over ad hoc wireless networks," *Proc. E-Activity and Leading Technologies Conference*, 2008, IASK, pp. 223-232.

[2] H. Osman and H. Taylor, "Managing group membership in ad hoc m-commerce trading systems," *Proc. 10th. Annual Intl Conference on New Technologies of Distributed Systems*, 2010, IEEE, pp. 173-180.

[3] H. Osman and H. Taylor, "Design of a reputation system for m-commerce by ad hoc networking," Technical Report, Dept. of Computer Science, Heriot-Watt University, 2010, pp. 1-7.

[4] A. Parkhe, "*Understanding trust in international alliances".* Journal of World Business, vol. 33, no. 3, 1998, Elsevier, pp. 219-240.

[5] P. Michiandi and R. Molva, "*Ad hoc networks security*," ST Journal of System Research, vol. 4, no. 1, 2003, pp. 756-775.

[6] Z. Liu, et al. "A dynamic trust model for mobile ad hoc networks," *Proc. 10th IEEE Intl Workshop on Future Trends of Distributed Computing Systems*, 2004, IEEE, pp. 80-85.

[7] L. Butyan, and J.-P. Hubaux, "Security and cooperation in wireless networks: Thwarting malicious and selfish behaviour in the age of ubiquitous computing," 2008, Cambridge University Press, pp. 74-77.

[8] J. Sen, P.R. Chowdhury, and S. Indranil, "A distributed trust establishment scheme for mobile ad hoc networks," *Proc. Intl Conference on Computing: Theory and Applications*, 2007. IEEE, pp. 51-58.

[9] P. Zimmermann, *Pretty Good Privacy User's Guide, Volume I* 1993. [cited 20/10/09]; Available from: http://www.tinyurls.co.uk/C19930

[10] P. Zimmermann, *Pretty Good Privacy User's Guide, Volume II* 1993. [cited 20/10/09]; Available from: http://www.tinyurls.co.uk/W19931

[11] A. A. Rahman, "*The PGP trust model*," 1996. [cited 01/07/09]: Available from: http://www.tinyurls.co.uk/H19926 , pp. 1-6.

[12] S. Capkun, L. Buttyan and J. Hubaux "*Self-organized public key management for mobile ad hoc networks*," IEEE Trans Mobile Computing, vol. 2, no. 1, 2003, IEEE, pp.52-64.

[13] A. Rachedi and A. Benslimane, "Trust and mobility-based clustering algorithm for secure mobile ad hoc networks," *Proc. Intl Conference on Systems and Networks Communication*, 2006, IEEE, pp. 72-77.

[14] E. C. H. Ngai and M. R. Lyu, "Trust and clustering-based authentication services in mobile ad hoc networks," *Proc. 24th. Intl Conference on Distributed Computing Systems Workshop*, 2004, IEEE, pp. 582-587.

[15] D. S. Thenmozhi and R. Murugan, "Security association in mobile ad hoc networks through self-organized public key certification," *Proc. 4th. Intl Conference on Applied Mathematics and Computer Science*, ACM, 2005. pp. 1-6.

[16] L. Cai, J. Pan, X. S. Shen and J. W. Mark, "*Promoting identity-based key management in wireless ad hoc networks*," Wireless Network Security, vol. 4, no. 2, 2007, Springer, pp. 83-102.

[17] B. Wu, et al. "*Secure and efficient key management in mobile ad hoc networks*," Journal of Network and Computer Applications, vol. 30, no. 3, 2007, Academic Press Ltd , pp. 937-954.

[18] M. Omar, Y. Challal and A. Bouabdallah, "*Reliable and fully distributed trust model for mobile ad hoc networks*," Computer and Security, vol. 28, no. 3-4, 2009, Elsevier, pp. 199-214.

References

[1] eBay Website, [cited 01/09/10]. available from: http://tinyurl.com/j2mlh.

[2] Zillow Website, [cited 30/01/16]. Available from: http://tinyurl.com/e4rmk.

[3] Nordstrom Website, [cited 30/01/16]. Available from: http://tinyurl.com/5zf6sj.

[4] Target Website, [cited 30/01/16]. Available from:http://tinyurl.com/j3nvcyc.

[5] SPIN Website, [cited 30/04/16]. Available from: http://spinroot.com.

[6] BPMN website, [cited 30/04/16]. available from: http://www.bpmn.org.

[7] A. Abdul-Rahman. The Pgp Trust Model. Electronic Resource, 1996. pages 1-6, Available from: http://tinyurl.com/lwlsfhc.

[8] K. Aberer and Z. Despotovic. Managing Trust in a Peer-to-Peer Information System. In *Proceedings of 10th. International Conference on Electronic and Knowledge Management*, pages 310–317. ACM, 2001.

[9] B. R. Adjei and S. A. Gouse. M-commerce Breakthrough in Developing Countries: the Role of M-commerce in Wealth Creation and Economic Growth in Developing Countries. Master's thesis, Department of Business Administration and Social Sciences, Division of Information Systems Sciences, Lulea University of Technology, 2006. pages 1-92.

[10] S. N. Ahmad. Business Models of P2P Companies: An Outlook of P2P Architecture Usage in Business Today. Electronic Article, 2003. Faculty of Economics and Management Sciences, Humboldt University Berlin.

[11] Y. Ai and F. Pang. Improved Pki Solution for Mobile Ad Hoc Networks. In *Proceedings of 2010 International Conference on Multimedia Technology (ICMT)*, pages 1–4. IEEE, 2010.

[12] R. A.Kale and S. R. Gupta. An Overview of MANET Ad Hoc Network. *International Journal Of Computer Science And Applications*, 6(2):223–227, 2013. Research Publications.

[13] N. Akhtar and M. Nauman. Timed-Automata Based Model-Checking of a Multi-Agent System: A Case Study. *Journal of Software Engineering and Applications*, 8:43–50, 2015. Scientific Research Publishing.

[14] S. A. K. Al-Omari and P. Sumari. An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Application. *Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks*, 2(1):87–110, 2010. Cornell University Library.

[15] L. Alvisi, J. Doumen, R. Guerraoui, B. Koldehofe, H. Li, R. van Renesse, and G. Tredan. How robust are gossip-based communication protocols? *ACM SIGOPS Operating Systems Review - Gossip-based Computer Networking*, 41(5):14–18, 2007. ACM New York.

[16] A. Amirat, A. Menasria, M. A. Oubelli, and N. Younsi. Automatic Generation of PROMELA Code from Sequence Diagram with Imbricate Combined Fragments. In *Second International Conference on Innovative Computing Technology (INTECH)*, pages 111–118. IEEE, 2012.

[17] F.-U. Andersen, H. de Meer, I. Dedinski, T. Hofeld, C. Kappler, A. Mder, J. O. Oberender, and K. Tutschku. An Architecture Concept for Mobile P2P File Sharing Services. In *Workshop at INFORMATIK 2004 - Algorithms and Protocols For Efficient Peer-To-Peer Applications*, pages 229–233. GI, 2004.

[18] A. S. Andreou, C. Chrysostomou, C. Leonidou, S. Mavromoustakos, A. Pitsillides, G. Samaras, and C. Schizas. Mobile Commerce Applications and Services: A Design and Development Approach. *International Journal of Mobile Communications*, 3(3):303–323, 2005. Inderscience Publishers.

[19] M. V. Arena, I. Blickstein, D. Gonzales, S. Harting, J. L. Lewis, M. M. M. McKernan, C. Nemfakos, J. Osburg, R. Rudavsky, and J. M. Sollinger. DoD and Commercial Advanced Waveform Developments and Programs with Multiple Nunn McCurdy Breaches, 2014. pages 1-112, RAND Corporation.

[20] K. Ashton. That "Internet of Things" Thing. *RFID Journal*, page 1, 2009. Date Available: 22/07/2009, Available from: http://www.rfidjournal.com/article/print/4986.

[21] S. Avancha, P. D'Souza, F. Perich, A. Joshi, and Y. Yesha. P2P M-Commerce in Pervasive Environments. *AIG SigeCom Exchanges*, 3(4):1–9, 2003.

[22] K. S. Barber, R. Mackay, and T.-H. Liu. Group Membership Services for Dynamically Organized Sensible Agent-Based Systems. In *Proceeding of the 12th. International FLAIRS Conference*, pages 160–165. AAAI, 1999.

[23] S. Barber, X. Boyen, E. Shi, and E. Uzun. Bitter to Better - How to Make Bitcoin a Better Currency. *Lecture Notes in Computer Science*, 7397:399–414, 2012. Springer-Verlag.

[24] S. J. Barnes. Under the Skin: Short-range Embedded Wireless Technology. *International Journal of Information Management*, 22(3):165–179, 2002. Elsevier.

[25] P. Benou and V. Bitos. Developing Mobile Commerce Applications. *Journal of Electronic Commerce in Organizations*, 6(1):63–78, 2008. IGI Global.

[26] K. P. Birman, M. Hayden, O. Ozkasap, Z. Xiao, M. Budiu, and Y. Minsky. Bimodal multicast. *ACM Transactions on Computer Systems*, 17(2):41–88, 1999. ACM.

[27] S. Boon and J. Holmes. *The Dynamics of Interpersonal Trust : Resolving Uncertainty in the Face of Risk. In Cooperation and Prosocial Behaviour.* Cambridge University Press, 1991.

[28] G. Breed. Wireless Ad Hoc Networks: Basic Concepts. *High Frequency Electronics*, pages 44–46, 2007. Summit Technical Media, LLC.

[29] E. Bulut. *Opportunistic Routing Algorithms in Delay Tolerant Networks.* PhD thesis, Faculty of Rensselaer Polytechnic Institute, Troy, New York, 2011. pages 1-157.

[30] G. Bykzkan. Determining the Mobile Commerce User Requirements Using an Analytic Approach. *Computer Standards & Interfaces*, 2008. Elsevier B.V.

[31] S. Capkun, L. Buttyn, and J.-P. Hubaux. Self-organized Public-Key Management for Mobile Ad Hoc Networks. *IEEE Trans Mobile Computing*, 2(1):52–64, 2003. IEEE.

[32] M. Carvalho. Security in Mobile Ad Hoc Networks. *IEEE Security and Privacy*, 6(2):72–75, 2008. IEEE.

[33] O. Cengiz. Adaptive Tactical Mesh Networking: Control Based MANET Model. Master's thesis, Naval Postgraduate School, Monterey, California, 2010. pages 1-45.

[34] Y.-C. Chang, J.-L. Chen, and W.-M. Tseng. A Mobile Commerce Framework Based on Web Services Architecture. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, volume 1, pages 403–408. IEEE Computer Society, 2005.

[35] J. Chase. The Evolution of the Internet of Things. White Paper, 2013. pages 1-7, Texas Instruments, Available from: http://www.ti.com/lit/ml/swrb028/swrb028.pdf.

[36] X. Chen and S. Lian. Service and P2P Based Secure Media Sharing in Mobile Commerce Environments. *Electronic Commerce Research*, 11(1):91–101, 2011. Springer Link.

[37] I. Chlamtac, M. Conti, and J. J.-N. Liu. Mobile Ad Hoc Networking: Imperatives and Challenges. *Ad Hoc Networls*, 1(1):13–64, 2003. Elsevier.

[38] C. Connolly, P. V. Dijk, F. Vierboom, and S. Wilson. Pki Interoperability models. *Galexia*, pages 1–23, 2005. Galexia Pty Ltd.

[39] M. Conti and Silvia. Multihop Ad Hoc Networking: The Theory. *IEEE Communications Magazine*, 45(4):78–86, 2007. IEEE.

[40] C. L. Corritore, B. Kracher, and S. Wiedenbeck. On-line Trust : Concepts, Evolving Themes, A Model. *International Journal of Human Computer Studies*, 58(3):737–758, 2003.

[41] M. S. Corson, J. P. Macker, and G. H. Cirincione. Internet-Based Mobile Ad Hoc Networking. *IEEE Internet Computing*, 3(4):63–70, 1999. IEEE.

[42] C. Coursaris and K. Hassanein. Understanding M-Commerce: A Consumer Centric Model. *Quaterly Journal of Electronic Commerce*, 3(3):247–271, 2002. Information Age Publishing, Inc.

[43] K. Cousins and U. Varshney. A Product Location Framework for Mobile Commerce Environment. In *Proceedings of the 1st international workshop on Mobile commerce*, pages 43–47. ACM, 2001.

[44] J. Craig and D. Jutla. *E-Business Readiness: A Customer-focused Framework*. Addison Wesley, 2000. pages 1-480.

[45] H. Dahshan and J. Irvine. Key Management in Web of Trust for Mobile Ad Hoc Networks. In *Proceedings of International Conference on Advanced Information Networking and Applications*, pages 363–370. IEEE, 2009.

[46] H. Dahshan and J. Irvine. A Robust Self-Organized Public Key Management for Mobile Ad Hoc Networks. *Security and Communications Networks,*, 3(1):16–30, 2010.

[47] A. Das and C. E. V. Madhavan. *Public-key Cryptography: Theory and Practice*. Pearson Education, 2009. pages 1-14.

[48] C. R. Davis. A Localized Trust Management Scheme for Ad Hoc Networks. In *3rd International Conference on Networking*, pages 671–675, 2004.

[49] C. de Morais Cordeiro, H. Gossain, and D. Agrawal. Multicast over Wireless Mobile Ad Hoc Networks: Present and Future Directions. *IEEE Network*, 17(1):52–59, 2003.

[50] K. S. Dhindsa and H. Aggarwal. Mobile Commerce : Standards & Design Technologies. *International Journal of Recent Trends in Engineering*, 2(4):92–95, 2009. Academy Publisher.

[51] D. Dutta, A. Goel, R. Govindan, and H. Zhang. The Design of a Distributed Rating Scheme for Peer-to-Peer Systems. In *Proceedings of 1st Workshop on Economic Issues in Peer to Peer Systems*, pages 1–5, 2003.

[52] G. F. Elmasry. *Tactical Wireless Communications and Networks: Design Concepts and Challenges*. John Wiley & Sons, Ltd., 2012. pages 205-224.

[53] D. Evans. The Internet of Things: How the Next Evolution of the Internet is Changing Everything. White Paper, 2011. pages 1-11, Cisco, Available from: http://tinyurl.com/88uhsx3.

[54] W. Ford and M. S. Baum. *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*. Prentice Hall, 2000. pages 1-640.

[55] C. E. Fossa and T. G. Macdonald. Internetworking Tactical MANETs. In *Military Communication Conference (MILCOM)*, pages 611–616. IEEE, 2010.

[56] P. Friess. *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, chapter Driving European Internet of Things Research, pages 1–6. River Publishers, 2013.

[57] M. Frodigh, P. Johansson, and P. Larsson. Wireless Ad Hoc Networkingthe Art of Networking Without a Network. *Ericson Review*, (4):248–263, 2000. Ericson.

[58] C. Gahlin. Secure Ad Hoc Networking. Master's thesis, Department of Computer Science, University of Umea, Sweden, 2004. pages 1-100, Available from: http://www8.cs.umu.se/ claes/thesis/.

[59] A. J. Ganesh, A.-M. Kermarrec, and L. Massoulie. Peer-to-peer Membership Management for Gossip-based Protocols. *IEEE Transactions on Computers*, 52(2):1–11, 2003.

[60] S. Ganu and D. Raychaudhuri. Integrating Short-Range Ad-Hoc Radio Technologies into Next-Generation Wireless Networks. In *Proceedings of the International Conference and Exposition on Communication and Computing*, pages 1–14. IEEE Press, 2005.

[61] H. M. Georges and W. Dong. Towards an Efficient Content-Based Dissemination Protocol and Notification Techniques for Disconnected MANETs. *International Journal of Information and Electronics Engineering*, 3(2):167–171, 2013. IJIEE.

[62] M. Gerla. From Battlefield to Urban Grids: New Research Challenges in Ad Hoc Wireless Networks. *Pervasive and Mobile Computing*, 1(1):78–93, 2005. Elsevier.

[63] A. Ghosh. *Security and Privacy for E-Business.* Wiley, 2001. pages 1-256.

[64] B. Gibbons. Mobile Commerce: Four Good Examples. Practicle Ecommerce Website, [cited 30/01/16], 2010. available from: http://tinyurl.com/yeekl9s.

[65] F. Glaser, K. Zimmerman, M. Haferkorn, M. C. Weber, and M. Siering. Bitcoin: - Asset or Currency? Revealing Users' Hidden Intentions. In *Twenty Second European Conference on Information Systems*, pages 1–14. Social Science Research Network (SSRN), 2014.

[66] R. Grinberg. Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal*, 4(1):160–207, 2011. Social Science Research Network (SSRN).

[67] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of Things (IoT): A Vision, Architectural Elements and Future Directions. *Future Generation Computer Systems*, 29:1645–1660, 2013. Elsevier.

[68] K. Hameed, K. Ahsan, and W. Yang. Mobile Commerce and Applications: An Exploratory Study and Review. *Journal of Computing*, 2(4):110–114, 2010.

[69] K. Hameed, H. Shah, K. Ahsan, and W. Yang. An Enterprise Architecture Framework for Mobile Commerce. *IJCSI International Journal of Computer Science*, 7(5):6–12, 2010.

[70] L. Han. Wireless Ad-hoc Networks. Technical report, Computer Science Department, Rutgers, The State University of New Jersey, USA, 2004. pages 1-6, Available from: http://tinyurl.com/pzjyvos.

[71] A. Hasti. Study of Impact of Mobile Ad Hoc Networking and its Future Applications. *BIJIT - BVICAMs International Journal of Information Technology*, 4(1):439–444, 2012. BIJIT.

[72] A. Heid. Analysis of the Cryptocurrency Marketplace. White Paper, 2013. pages 1-35, HackMiami, Available from: http://www.hackmiami.org.

[73] D. Helen and D. Arivazhagan. Applications, Advantages and Challenges of Ad Hoc Networks. *Journal of Academia and Industrial Research*, 2(8):453–457, 2014. JAIR.

[74] T. Hofeld, K. Tutschku, and F.-U. Andersen. Mapping of File-Sharing onto Mobile Environments: Enhancement by Umts. In *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, pages 43–49. IEEE, 2005.

[75] G. J. Holzmann. The model checker spin. *IEEE Transactions on Software Engineering*, 23(5):279–295, 1997. ACM Digital Library.

[76] W.-C. Hu, C.-W. Lee, and J.-H. Yeh. *Mobile Commerce Applications*, chapter Mobile Commerce Systems, pages 2–23. Idea Group Inc., 2004.

[77] W.-C. Hu, C.-H. T. Yang, J.-H. Yeh, and W. Hu. Mobile and Electronic Commerce Systems and Technologies. *Journal of Electronic Commerce in Organizations*, 6(3):54–73, 2008. IGI Global.

[78] S. Huang, D. MacCallum, and D. Z. Du. Routing Security in Ad Hoc Wireless Networks. *Network Security*, pages 1–32, 2005. Springer.

[79] J.-P. Hubaux, L. Buttyn, and S. Capkun. The Quest for Security in Mobile Ad Hoc Networks. In *Proceedings of the 2nd ACM Interational Symposium on Mobile Ad Hoc Networking and Computing*, pages 146–155. ACM, 2001.

[80] IETF. Mobile Ad Hoc Networks Working Group. Website, Date Established: 1997. http://www.ietf.org/html.charters/manetcharter. html.

[81] I. Ismail and M. H. F. Jaafar. Mobile Ad Hoc Network Overview. In *2007 Asia-Pacific Conference on Applied Electromagnetics*, pages 1–8. IEEE, 2007.

[82] V. P. Jacob. M-Commerce: Myth or Reality? *Delhi Business Review*, 3(1), 2002.

[83] E. Jacobs. Bitcoin: A Bit Too Far. *Journal of Internet Banking and Commerce*, 16(2):1–4, 2011. JIBC Publisher.

[84] A. Josang. The Right Type of Trust for Distributed Systems. In *Proceedings of the 1996 Workshop on New Security Paradigms*, pages 119–131. ACM, 1996.

[85] A. Jsang, R. Ismail, and C. Boyd. A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, 43(2):618–644, 2007. Elsevier.

[86] R. Jurca and B. Faltings. An Incentive Compatible Reputation Mechanism. In *Proceeding of the IEEE Conference on E-Commerce*, pages 285–292. IEEE, 2003.

[87] K. Karimi and G. Atkinson. What the Internet of Things (IoT) Needs to Become a Reality. White Paper, 2013. pages 1-15, Freescale, Available from: http://tinyurl.com/q7h74o7.

[88] S. Kerremans. Ad Hoc Networks and the Future of Mobile Network Operators. Master's thesis, Department of Industrial Engineering and Innovation Sciences, 2011. pages 1-289.

[89] S. H. Kim. Impact of Mobile-Commerce: Benefits, Technological and Strategic Issues and Implementation. *Journal of Applied Sciences*, 6(12):2523–2531, 2006.

[90] F. Kritzinger and D. Truter. A Secure End-to-End System for M-Commerce. Technical report, Department of Computer Science, University of Cape Town, 2003. pages 1-11, Available from: http://tinyurl.com/nzudm7y.

[91] B. S. T. Lai. Trust in Online Trading Systems. Master's thesis, University of Auckland, 2004. pages 1-151.

[92] C.-H. Lee and D. Y. Eun. Exploiting Heterogeneity in Mobile Opportunistic Networks: An Analytic Approach. In *Proceeding of IEEE SECON*, pages 502–510. IEEE, 2010.

[93] J. A. Lehtinen. Design and Implementation of Mobile Peer-to-Peer Application. Master's thesis, Department of Electrical and Communications Engineering, Networking Laboratory, Helsinki University of Technology, 2006. pages 1-89.

[94] X. Li, S. Gordon, and J. Slay. On Demand Public Key Management for Wireless Ad Hoc Networks. In *Conference on Global Telecommunications*, pages 1284–1289, 2004.

[95] X. Li and W. Kou. A Secure M-Commerce Model Based on Wireless Local Area Network. In *Proceedings of the 18th International Conference on Advanced Information Networking and Application*. IEEE Computer, 2004.

[96] Q. Lian, Z. Zhang, M. Yang, B. Zhao, Y. Dai, and X. Li. An Empirical Study of Collusion Behavior in the Maze P2P File-Sharing System. In *Proceedings of the 27th International Conference on Distributed Computing Systems*, page 56. IEEE Computer Society, 2007.

[97] A. Lindgren, K. S. Phanse, T. Johansson, R. Brannstrom, and C. Ahlund. Future Directions in Ad Hoc Networking Research. In *5th Scandinavian Workshop on Wireless Ad-hoc Networks*, pages 1–5, 2005.

[98] P. D. Linh. A Study for Peer-to-Peer File-Sharing Application in Cellular Mobile Networks. Master's thesis, Graduate School of Global Information and Telecommunication Studies, Waseda University, 2010. pg. 1-48.

[99] J. Linn. Trust Models and Management in Public-Key Infrastructures. Electronic Articles, 2000. pages 1-13, RSA Laboratories, Bedford, USA, Available from: http://tinyurl.com/pqzur5f.

[100] J. Liu, D. Sacchetti, F. Sailhan, and V. Issarny. Group Management for Mobile Ad Hoc Networks: Design, Implementation and Experiment. In *Proceeding of 6th. International Conference on Mobile Data Management*, pages 192–199. ACM, 2005.

[101] S. Maffei. M-Commerce Needs Middleware! Electronic Article, pages 1-6, 2001. Available from: http://tinyurl.com/l3j8y4q.

[102] S. Maki, T. Aura, and M. Hietalahti. Robust Membership Management for Ad-Hoc Groups. In *Proceeding of 5th Nordic Workshop on Secure IT Systems*, pages 1–18, 2000.

[103] R. Mangla. Mobile Ad Hoc Networks. *International Journal of Educational Administration*, 2(4):697–706, 2010. Research India Publications.

[104] S. Marti and H. Garcia-Molina. Limited Reputation Sharing in P2p Systems. In *Proceeding of the 5th. ACM Conference on Electronic Commerce*, pages 91–101. ACM, 2004.

[105] R. C. Mayer, J. H. Davis, and F. D. Schoorman. An Integrative Model of Organizational Trust. *Academy of Management Review*, 20(3):709–734, 1995. JSTOR.

[106] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. B. Srivastava. Coverage Problems in Wireless Ad-hoc Sensor Networks. In *IEEE Infocom*, pages 1380–1387. IEEE, 2001.

[107] Q.-A. Minhas, H. Mahmood, and H. Malik. *Recent Developments in Mobile Communications in A Multidisciplinary Approach: The Role of Ad Hoc Networks in Mobile Telecommunication*. Intech, 2011. pages 179-200.

[108] M. Munusamy and H. P. Leang. Characteristics of Mobile Devices and an Integrated M-commerce Infrastructure for M-commerce Deployment. In *4th. International Conference on Electronic Commerce*, pages 1–10, 2002.

[109] C. S. R. Murthy and B. S. Manoj. *Ad Hoc Wireless Networks: Architectures and Protocol*. Prentice, 2004. pages 191-230.

[110] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. *Consulted 1*, 28(2012):1–9, 2008. Available from: https://bitcoin.org/bitcoin.pdf.

[111] E. Ngai and A. Gunasekaran. A Review for Mobile Commerce Research and Applications. *Decision Support Systems*, 43(1):3–15, 2007. Elsevier.

[112] H. A. Nguyen and S. Giordano. Routing in Opportunistic Networks. *International Journal of Ambient Computing and Intelligence (IJACI)*, 1(3):19–38, 2009. IGI Global.

[113] A. Nisbet. The Challenges in Implementing Security in Spontaneous Ad Hoc Networks. In *Proceedings of 13th. Australian Information Security Mangement Conference*, pages 112–119. Research Online, 2015.

[114] Nokia. Connecting Mobile Consumers and Merchants. White Paper, 2004. Available from: http://tinyurl.com/p29l3e8.

[115] J. O. Oberender, F.-U. Andersen, H. de Meer, I. Dedinski, T. Hofel, C. Kappler, A. Mader, and K. Tutschku2. Enabling Mobile Peer-to-Peer Networking. In *Wireless Systems and Mobility in Next Generation Internet of Lecture Notes in Computer Science*, volume 3427, pages 219–234. Springer Link, 2005.

[116] E. A. Oladimeji, S. Supakkul, and L. Chung. Security Threat Modeling and Analysis: A Goal-Oriented Approach. In *10th IASTED International Conference on Software Engineering and Applications*, pages 13–15. IASTED, 2006.

[117] H. Osman and H. Taylor. Towards a Reference Model for M-commerce over Ad Hoc Wireless Networks. In *Proceedings of E-Activity and Leading Technologies (E-ALT) Conference*, pages 223–232. IASK, 2008.

[118] H. Osman and H. Taylor. Managing Group Membership in Ad Hoc M-commerce Trading Systems. In *Proceedings of 10th. Annual International Conference on New Technologies of Distributed Systems*, pages 173–180. IEEE, 2010.

[119] H. Osman and H. Taylor. Identity Support in a Security and Trust Service for Ad Hoc M-commerce Trading Systems. In *Proceedings of 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA)*, pages 285 – 290. IEEE, 2011.

[120] A. Parkhe. Understanding Trust in International Alliances. *Journal of World Business*, 33(3):219–240, 1998. Elsevier.

[121] V. Patil and R. K. Shyamasundar. Trust Management for E-Transactions. *Sadhana*, 30(2 and 3):141–158, 2005. Indian Academy of Science.

[122] A. Penttinen. Research on Ad Hoc Networking: Current Activity and Future Directions. CiteSeerX, 2007. pages 1-10, ScientificCommons.

[123] F. Perich, A. Joshi, and Y. Yesha. Neighborhood-Consistent Transaction Management for Pervasive Computing Environment. In *14th. International Conference on Database and Expert Systems Applications*, pages 1–10. UMBC Ebiquity Research Group, 2003.

[124] K. S. Phanse and J. Nykvist. Opportunistic Wireless Access Networks. In *Proceedings of the 1st International Conference on Access Networks*, number 11, pages 1–5. ACM New, 2006.

[125] W. T. Polk and N. E. Hastings. Bridge Certification Authorities: Connecting B2b Public Key Infrastructures. Electronic Article, 2000. pages: 1-14, National Institute of Standards and Technology.

[126] P. Pradan and A. Helal. An Efficient Algorithm for Maintaining Consistent Group Membership in Ad Hoc Networks. In *Proceeding of 23rd International Conference on Distributed Computing Systems*, pages 428–433. IEEE Computer Society, 2003.

[127] S. Pradhan, E. Lawrence, and A. Zmijewska. Bluetooth as an Enabling Technology in Mobile Transactions. In *Proceedings of the International Conference on Information Technology: Coding and Computing*. IEEE Computer Society, 2005.

[128] S. Rahamatkar, A. Agarwal, and A. Singh. Mobile Middleware and Integrated Structure for Emerging Wireless Commerce Applications. *International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS)*, 1(2):284–292, 2009.

[129] M. Rajni and Ms.Reena. Review of MANETS Using Distributed Public-key Cryptography. *International Journal of Computer Trends and Technology (IJCTT)*, 10(3):143–147, 2014. arXiv preprint.

[130] R. Ramanathan, R. Allan, P. Basu, J. Feinberg, G. Jakllari, V. Kawadia, J. R. S. Loos, C. Santivanez, and J. Freebersyser. Scalability of Mobile Ad Hoc Networks: Theory vs Practice. In *The 2010 Military Communications Conference (MILCOM 2010)*, pages 493–498. IEEE, 2010.

[131] R. Ramanathan and J. Redi. A Brief Overview of Ad Hoc Networks: Challenges and Directions. *IEEE Communications Magazine*, 50th Anniversary Commemorative Issue:20–22, 2002.

[132] C. Ranganathan and S. Ganapathy. Key Dimensions of Business-to-consumer Web Sites. *Information & Management*, 39(6):457–465, 2002. Elsevier.

[133] M. Raya and J. P. Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proceedings of the 3rd. ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 11–21. ACM, 2005.

[134] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman. Reputation Systems. *Communications of the ACM*, 43(12):45–48, 2000. ACM.

[135] Ritu and M. K. Sidhu. Routing Protocols in Infrastructure-less Opportunistic Networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(6):1318–1322, 2014. IJARCSSE.

[136] G. Roman, Q. Huang, and A. Hazemi. On Maintaining Group Membership Data in Ad Hoc Networks. Technical Report WUCS-00-26, Washington University, 2000. pages. 1-11.

[137] R.Rajkumar, N.Ch.S.N.Iyengar, and D.Saikrishna. Architecture for Mobile P2P Auction using JXTA/JXME in M-Commerce. *International Journal of Advanced Engineering Sciences and Technologies*, 4(2):4–9, 2011.

[138] C. Satizabal, R. Paez, and J. Forne. Pki Trust Relationships: from a Hybrid Architecture to a Hierarchical model. In *Proceedings of the first International Conference on Availability, Reliability and Security*, pages 1–8. IEEE Computer Society, 2006.

[139] B. Schoenmakers. Basic Security of the e-cash Payment System. *Lecture Notes in Computer Science*, 1538:338–352, 1997. Springer-Verlag.

[140] S. Schwiderski-Grosche and H. Knospe. Secure M-Commerce. Electronic Article. [cited 15/06/07], pages 1-15, Available from: http://tinyurl.com/pw3nxfg.

[141] H. Shi, W. Ma, M. Yang, and X. Zhang. A Case Study of Model Checking Retail Banking System with SPIN. *Journal of Computer*, 7(10), 2012. Academy Publisher.

[142] R. Shim and V. Rice. How to Unwire your Business. *Technology Review, Special Issue of Fortune*, pages 46–54, 2001. ZDNet.

[143] D. Shinder. Understanding the Role of the PKI. Electronic Articles, 2003. [cited:12/01/12], Available from: http://tinyurl.com/bs2wchr.

[144] K. Siau, E.-P. Lim, and Z. Shen. *Advances in Mobile Commerce Technologies*, chapter Mobile Commerce: Current States and Future Trends, pages 1–17. Idea Group Inc. (IGI), 2003.

[145] M. L. Srinivasan. Public Key Infrastructure (PKI) and other Concepts in Cryptography for CISSP Exam. Electronic Article, 2008. [cited: 12/01/12], Available from: http://tinyurl.com/ykflhkn.

[146] I. Staff. The Future of Cryptocurrency. Electronic Article, 2013. pages 1-3, Date published: 10/09/13, Available from: http://tinyurl.com/ojlzz59.

[147] K. Stanoevska-Slabeva. Towards a Reference Model for M-commerce Applications. In *XIth. European Conference on Information Systems*, pages 1–13. AIS Electronic Library, 2003.

[148] M. Steiner, G. Tsudik, and M. Waidner. Key Agreement in Dynamic Peer Groups. *IEEE Transactions on Parallel and Distributed Computing*, 11(8):769–780, 2000. IEEE.

[149] D. R. Stephens, C. Magsombol, and N. Browne. Network Programming of Joint Tactical Radio System Radios. In *2008 IEEE Military Communications Conference (MILCOM 2008)*, pages 1–6. IEEE, 2008.

[150] J.-Z. Sun. Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing. In 3, editor, *Proceedings of International Conferences on Infotech & Infonet*, pages 316–321. IEEE, 2001.

[151] W. Sun, M. Choi, and S. Choi. IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz. *Journal of ICT Standardization*, 1:83–108, 2013. River Publishers.

[152] K. Taneja and R. B. Patel. Mobile Ad Hoc Networks: Challenges and Future. In *Proceedings of National Conference on Challenges & Opportunities in Information Technology*, pages 133–135, 2007.

[153] P. Tarasewich, R. C. Nickerson, and M. Warkentin. Issues in Mobile E-Commerce. *Communication of the Association for Information Systems*, 8(3):41–46, 2002.

[154] P. Tarasewich, R. C. Nickersonand, and M. Warkentin. Wireless/Mobile E-Commerce:Technologies, Applications, and Issues. In *7th Americas Conference on Information Systems*, pages 435–438. AIS Electronic Library (AISeL), 2001.

[155] P. Thompson, A. James, and L. Smalov. Sharing Design Information Using Peer-to-Peer Computing. *Lecture Notes in Computer Science (Computer Supported Cooperative Work in Design III)*, 4402:73–81, 2007. Springer Link.

[156] R. Tiwari, S. Buse, and C. Herstatt. From Electronic to Mobile Commerce: Opportunities Through Technology Convergence for Business Services. *Asia*

Pacific Tech Monitor, 23(5):38–45, 2006. Social Science Research Network (SSRN).

[157] R. Tiwari, S. Buse, and C. Herstatt. The Mobile Commerce Technologies: Generations, Standards and Protocols. Technical report, Hamburg University of Technology, Institute of Technology and Innovation Management, 2006. pages 1-21, http://ssrn.com/abstract=1583453.

[158] C. K. Toh. *Ad Hoc Mobile Wireless Networks: Protocols and Systems*. Prentice Hall, 2001. pages 19-26.

[159] A. Tsalgatidou and E. Pitoura. Business Models and Transactions in Mobile Electronic Commerce: Requirements and Properties. *Computer Networks*, 37(2):221–236, 2001. Elsevier.

[160] A. Tsalgatidou and J. Veijalainen. Mobile Electronic Commerce: Emerging Issues. In *Proceedings of the First International Conference on Electronic Commerce and Web Technologies*, pages 477–486. Springer, 2000.

[161] A. Tsalgatidou and J. Veijalainen. Requirements for Mobile E-Commerce. In *Proceedings of the E-business and E-work Conference*, pages 1–7, 2000.

[162] E. Turban and D. King. *Introduction to E-Commerce*. Prentice Hall, 2003. pages 336-337.

[163] J. van der Merwe, D. Dawoud, and S. McDonald. Fully Self-Organized Peer-to-Peer Key Management for Mobile Ad Hoc Networks. In *Proceedings of the 4th ACM Workshop on Wireless Security*, pages 21–30. ACM, 2005.

[164] U. Varshney. Business Models for Mobile Commerce Services: Requirements, Design, and the Future. *IT Proffesional*, 10(6):48–55, 2008. IEEE Computer Society.

[165] U. Varshney and R. Vetter. A Framework for the Emerging Mobile Commerce Applications. In *Proceedings of the 34th. Hawaii International Conference on System Sciences*, pages 1–6. IEEE, 2001.

[166] U. Varshney and R. Vetter. Mobile Commerce: Framework, Applications and Networking Support. *Mobile Networks and Applications*, 7(3):185–198, 2002. Kluwer Academic Publishers.

[167] J. Veijalainen, V. Terziyan, and H. Tirri. Transaction Management for M-commerce at a Mobile Terminal. In *Proceedings of the 36th. Annual Hawaii International Conference on System Sciences*, pages 89–98. IEEE, 2003.

[168] Verisign. Introduction to Digital Certificates. Electronic Article. [cited: 10/01/12], Available from: http://tinyurl.com/ybx4xwt.

[169] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, and P. Doody. *Internet of Things - Global Technological and Societal Trends*, chapter Internet of Things Research Agenda, pages 9–50. River, 2011.

[170] N. Vimala and D. R. Balasubramaniam. Distributed Key Management Scheme for Mobile Ad-Hoc Network - A Survey. *Global Journal of Computer Science and Technology*, 10(2):7–11, 2010.

[171] B. Wu, J. Chen, J. Wu, and M. Cardei. A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. *Wireless /Mobile Network Security*, pages 1–38, 2006. Springer.

[172] L. Xiong and L. Liu. A Reputation-based Trust Model for Peer-to-Peer E-commerce Communities. In *Proceedings of IEEE Conference on E-Commerce*, pages 275–284. IEEE, 2003.

[173] B. Xu and S. Hischke. The Role of Ad Hoc Networking in Future Wireless Communications. In *International Conference on Communication Technology*, volume 2, pages 1353 – 1358. IEEE, 2003.

[174] Z. Yan and S. Holtmanns. *Trust Modeling and Management: From Social Trust to Digital Trust in Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions.* Idea Group Inc., 2008.

[175] M. K. Yogi and V. Chinthala. A Study of Opportunistic Networks for Efficient Ubiquitous Computing. *International Journal of Advanced Research in Computer and Communication Engineering*, 3(1):5187–5191, 2014. IJARCCE.

[176] B. Yu and M. P. Singh. Distributed Reputation Management for Electronic Commerce. *Computational Intelligence*, 18(4):535–549, 2002.

[177] Z. Yu, F. Zhiyuan, and L. Ning. A Peer-to-Peer e-Market Organized within Mobile Devices Based on Distributed Services. In *IEEE International Conference on e-Business Engineering*, pages 633–636. IEEE, 2008.

[178] M. G. Zapata. Key Management and Delayed Verification for Ad Hoc Networks. *Journal of High Speed Networks*, 15(1):93–109, 2006. IOS Press.

[179] H. Zhai, J. Wang, X. Chen, and Y. Fang. Medium Access Control in Mobile Ad Hoc Networks: Challenges and Solutions. *Wireless Communications and Mobile Computing*, 6(2):151–170, 2006. Wiley-Blackwell.

[180] J. J. Zhang, Y. Yuan, and N. Archer. Driving Forces for M-Commerce Success. *E-Business Management Integrated Series in Information Systems*, 1:51–76, 2002. Springer Link.

[181] L. Zhao and X. Feng. The M-Commerce Architecture Study Based on Saas Model. In *International Conference on Management and Science*, pages 1–4. IEEE Explore, 2009.

[182] P. Zheng and L. Ni. *Smart Phone and Next Generation Mobile Computing*. Morgan Kaufmann, 2005. pages 469-471.

[183] L. Zhou and Z. J. Haas. Securing Ad Hoc Networks. *IEEE Network*, 13(6):24–30, 1999. IEEE.

[184] P. Zimmermann. Pretty Good Privacy User's Guide, Volume I. Electronic Resource, 1993. Available from: http://tinyurl.com/32wjvqc.

[185] P. Zimmermann. Pretty Good Privacy User's Guide, Volume II. Electronic Resource, 1993. Available from: http://tinyurl.com/pl6492f.