Security Management for Mobile Ad hoc Network of Networks (MANoN)

PhD Thesis

Ali Hilal Al-Bayatti

This thesis is submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

Software Technology Research Laboratory (STRL)
Faculty of Technology
De Montfort University

February 2009

DEDICATION

To My Beloved Father

Prof. Dr. Hilal Mohammed Al-Bayatti

Who without him the PhD dream would not be a reality

For his endless support, encouragement and love all the way through my life.

To My Loving Mother

Mariam Murrad Al-Waisy

For everything she sacrificed in her life for me.

Abstract

Mobile Ad hoc Network of Networks (MANoN) are a group of large autonomous wireless nodes communicating on a peer-to-peer basis in a heterogeneous environment with no pre-defined infrastructure. In fact, each node by itself is an ad hoc network with its own management. MANoNs are evolvable systems, which mean each ad hoc network has the ability to perform separately under its own policies and management without affecting the main system; therefore, new ad hoc networks can emerge and disconnect from the MANoN without conflicting with the policies of other networks. The unique characteristics of MANoN makes such networks highly vulnerable to security attacks compared with wired networks or even normal mobile ad hoc networks.

This thesis presents a novel security-management system based upon the Recommendation ITU-T M.3400, which is used to evaluate, report on the behaviour of our MANoN and then support complex services our system might need to accomplish. Our security management will concentrate on three essential components:

- *Security Administration*
- *Prevention and Detection*
- *Containment and Recovery*

In any system, providing one of those components is a problem; consequently, dealing with an infrastructure-less MANoN will be a dilemma, yet we approached each set group of these essentials independently, providing unusual solutions for each one of them but concentrating mainly on the prevention and detection category.

The contributions of this research are threefold. First, we defined ***MANoN Security Architecture*** based upon the ITU-T Recommendations: X.800 and X.805. This security architecture provides a comprehensive, end-to-end security solution for MANoN that could be applied to every wireless network that satisfies a similar scenario, using such networks in order to predict, detect and correct security vulnerabilities. The security architecture identifies the security requirements needed, their objectives and the means by which they could be applied to every part of the MANoN, taking into consideration the different security attacks it could face.

Second, realising the prevention component by implementing some of the security requirements identified in the Security Architecture, such as *authentication*, *authorisation*, *availability*, *data confidentiality*, *data integrity* and *non-repudiation* has been proposed by means of defining a novel ***Security Access Control Mechanism*** based on ***Threshold Cryptography Digital Certificates*** in MANoN.

Network Simulator (NS-2) is a real network environment simulator, which is used to test the performance of the proposed security mechanism and demonstrate its effectiveness. Our ACM-MANoN results provide a ***fully distributed*** security protocol that provides ***a high level of secure, available, scalable, flexible and efficient*** management services for MANoN.

The third contribution is realising the detection component, which is represented by providing a ***Behavioural Detection Mechanism*** based on nodes behavioural observation engaged with policies. This behaviour mechanism will be used to detect malicious nodes acting to bring the system down. This approach has been validated using an attacks case study in an unknown military environment to cope with misbehaving nodes.

Declaration

I declare that the work described in my thesis is original work undertaken by me for the degree of Doctor of Philosophy, at Software Technology Research Laboratory (STRL), at De Montfort University, United Kingdom.

No part of the material described in this thesis has been submitted for the award of any other degree or qualification in this or any other university or college of advanced education.

Ali Hilal Al-Bayatti

ACKNOWLEDGEMENTS

First and Foremost, my deepest thankfulness goes to the most merciful **ALLAH** for all his blessings and bounties he gave me since I was born, without his blessings I would not be in this place at all.

Most importantly, I would like to express my sincere gratitude to my supervisor, **Professor Hussein Zedan**, without his support, patients and guidance this thesis would have been impossible to achieve. I was fortunate enough to have him by my side, meetings with him was enjoyable and discussions were insightful. The only thing I can say to him is thank you for everything.

Also, I wish to thank my supervisor *Dr. Antonio Cau* for his professional guidance and critical comments which helped to improve my technical writing. I also want to thank *Dr. François Siewe* for his technical suggestions and guidance to improve this thesis.

Special appreciation goes to *Dr. Iman Almomani* for her significant support and insightful comments through the earliest phase of my research.

I am deeply indebt to my father and mentor **Professor Hilal Al-Bayatti** who was and still behind everything I have learned and achieved in my life. He made sure that I was never bothered with any responsibilities other than my research. I owe everything I have to him. I love to express my deepest gratitude to my **Mother**, for her care, patience, support, prayers and for the endless nights she was looking after me. Without her, I am nothing. Also, I love to thank my lovely sisters *Rasha* and *Rana* for their love, concern and engorgement along the way. My parents you made this work possible through all your love, patience, generosity and understanding. My gratitude is inexpressible. I could not possibly give back to you what you have lost to support me. I am trying to honour your sacrifice. I am dedicating this thesis to you with love and respect.

I would like to thank all my colleagues at the Software Technology Research Laboratory group – De Montfort University for their constant support and making STRL such a simulating and friendly environment for research.

Last but not least, big gratitude goes to my friend and brother *Dr. Mohammed Taye* for all his encouragement and advices. Our friendship started here and will last forever. Also I wish to thank my dearest and best friends *Manar Yusur, Moqdad Khalid, Mostafa Saed and Mudher Issa* for all the encouragement and nice words they gave me all these years.

PUBLICATIONS

1. **Ali H. Al-Bayatti, H. Zedan, A. Cau, "*Security Solution for Mobile Ad Hoc Network of Networks (MANoN)*", IEEE Fifth International Conference of Networking and Services ICNS, pp. 255 – 262, April 2009.**

2. **Ali H. Mohammed, H. Zedan, and A. Cau, "*Security Architecture for MANoN*", Proceedings of IDIAS 2008, April 2008.**

TABLE OF CONTENT

LIST of Tables

LIST of Figures

List of Acronyms

ACM	Access Control Mechanism
ACL	Access Control List
AES	Advanced Encryption Standard
AODV	Ad hoc On-demand Distance Vector
ARAN	Authenticated Routing protocol for Ad hoc Network
ARPA	Advanced Research Project Agency
ARIADNE	A Secure On-Demand Routing for Ad hoc Network
ATI	Authentication Time Interval
BBN	Back Bone Node
BD	Behaviour Detection
CA_{Se}	Certificate Authority Servers
CA_{C}	Certificate Authority Combiner
CA	Certificate Authorities
CH	Cluster Head
CRL	Certificate Revocation List
DAC	Discretionary Access Control
DARPA	Defence Advanced Research Project Agency
DC	Data Collector
DCF	Distributed Coordination Function
DNS	Domain Name Service
DoS	Denial of Service
DSDV	Destination Sequence Distance Vector
DSR	Dynamic Source Routing
DSSS	Direct-Sequence Spread Spectrum

FCAPS	Fault-management, Configuration, Accounting, Performance and Security
FHSS	Frequency-Hopping Spread Spectrum
GBBN	Global Back Bone Node
GN	General Node
IDS	Intrusion Detection System
IFQ	Interface Queue
IPS	Intrusion Prevention System
IR	Infrared
ITU-T	Institute Technology Union- Telecommunication Standardization Sector
LBBN	Local Back Bone Node
LDB	Local Data Base
LL	Link Layer
MAC	Medium Access Control
MAC	Mandatory Access Control
MANET	Mobile Ad hoc Network
MANoN	Mobile Ad hoc Network of Networks
NATO	North Atlantic Treaty Organisation
MOCA	Mobile Certificate Authority
MP	MOCA Protocol
NIST	National Institute of Standards and Technology
NoN	Network of Networks
NS-2	Network Simulator 2
OAM&P	Operation, Administration, Maintenance and Provisioning
OSI	Open System Interconnection
OTCL	Object-oriented extension of TCL
P	Public Key
PAN	Personal Area Network

PC	Personal computer
PGP	Pretty Good Privacy
PK	Public Key
PKI	Public Key Infrastructure
Pr	Private Key
QoS	Quality of Service
RA	Reputation Assistant
RA	Registration Authority
RAM	Reputation Assistant Mechanism
RBAC	Role Based Access Control
RF	Radio Frequency
RIT	Route Information Table
RREP	Route Reply
RREQ	Route Request
RPC	Remote Procedure Call
RWP	Random WayPoint
SAR	Security Aware ad hoc Routing protocol
SEAD	Secure Efficient Ad hoc Distance vector Routing
SK	Private Key
SMT	Secure Message Transmission
SN	Sequence Number
SoS	System of Systems
TCP	Transmission Control Protocol
TTP	Trusted Third Party
UK	United Kingdom
URSA	Ubiquitous and Robust Access Control
US	United States
VINT	Virtual InterNetwork Testbed
WLAN	Wireless Local Aria Network

WoT	Web of Trust
Z-H	Zhou and Haas

Chapter 1

Introduction

1.1 Research Motivations

The aims of wireless technology meet the need for fast, reliable and secure information exchange, communication networks in the future have become an integral part of our society. The success of any corporation depends largely upon its ability to communicate. The emerging MANoN technology attempt to offer users with anytime and anywhere services in a large heterogeneous infrastructure-less wireless network, based on collaboration between individual network nodes. In the last few years, there has been considerable interest in MANoNs, as they have significant potential in military situations, such as disaster recovery situations and rescue missions, and in commercial, smart homes and academic institutions such as class/conference room applications.

The unique characteristics of MANoN are decentralised decision making (lack of central authority), policy conflicts, dynamic changing topology, short range connectivity, shared radio channel, limited resource availability and physical vulnerability which make such networks highly vulnerable to security attacks compared with wired, infrastructure-based wireless networks or even normal Mobile Ad hoc Networks (MANET).

Consequently, the main challenge facing MANoN is security, in precise security management that needs deep investigation and proper solutions. Providing security management is considered to be the most crucial solution to the MANoN security problem, since MANoN deals with different aspects such as providing efficient key management, routing and security administration especially prevention and detection techniques. In addition, a successful security management system represented by providing proper prevention and detection techniques will ensure the implementation of most of the security requirements such as *authentication*, *authorisation*, *data confidentiality*, *data integrity* and *non-repudiation*.

1.2 Problem Statement and Security Solutions

Based on the growing demands of military and industrial projects for evolvable systems [101, 102], our state-of-the-art MANoN is an excellent solution to those demands, as it deals with multi wireless *ad hoc* networks under its own policies, regulations and management in a heterogeneous environment, with no pre-defined infrastructure; each ad hoc network has the ability to emerge or disconnect without affecting the main MANoN system. Nevertheless, providing these types of systems is one thing and providing security is another. Therefore, such networks are highly vulnerable to security attacks compared with wired networks or even normal mobile ad hoc networks.

In general, MANoN faces major issues and challenges that need to be considered when designing this type of network. Security is our main concern and the focus of this research. We found that providing security management is a proper solution required by any system, and our system is not exempted from this network policy.

Before discussing the essential aspects of security management, we need to design a comprehensive security foundation/architecture upon which to implement our security requirements. Hence, we designed a security architecture based upon the ITU-T Recommendations, X.800 and X.805 [56, 57], which provides a comprehensive, bottom-up, end-to-end security solution for MANoN that could be applied to every wireless network that satisfies a similar scenario using such networks in order to predict, detect and correct security vulnerabilities. The security architecture identifies the security requirements needed, their objectives and the means by which they could be applied to every part of the MANoN, taking into consideration the different kinds of security attack it could face.

In order to achieve the objectives of the security requirements defined in the security architecture for MANoN, a set of mechanisms must be proposed to enforce these security requirements and forestall any attempts to evade them.

Various technologies can be applied to implement the security requirements. Modern cryptography – including public key cryptography, digital signatures and digital certificates – are the most powerful tools that can be used to implement most of the security requirements, including *authentication, authorisation, data confidentiality, data integrity* and *non-repudiation.*

In fact, cryptography techniques are part of the essential security management tools as they fall into the *Prevention and Detection* component [59]. This category is one of the central aspects of security management in MANoN, which requires effective mechanisms in order to achieve and implement the defined security requirements.

We realised the prevention component by implementing some of the security requirements identified in the Security Architecture, such as *authentication, authorisation, availability, data confidentiality, data integrity* and *non-repudiation,* that have been proposed by means of defining a novel ***Security Access Control Mechanism based on Threshold Cryptography Digital Certificates*** in MANoN. Moreover, we evaluated our security mechanism by the Network Simulator (NS-2), which is a real network environment simulator used to test the performance of the proposed security mechanism and demonstrate its effectiveness.

Furthermore, we implemented a detection component, which is represented by providing a ***Behavioural Detection Mechanism*** based on nodes behaviour compared with our system policies. This behaviour mechanism will be used to detect malicious nodes acting to bring the system down. This approach has been validated using a proper formalisation and an attacks case study to cope with misbehaving nodes.

1.3 Original Contributions

This thesis makes the following main original contributions.

Security Architecture for MANoN: A security architecture is proposed that provides the specification of a comprehensive, end-to-end security solution for a MANoN that could be applied to every wireless service provisioning scenario using this type of network in order to detect, predict and correct security vulnerabilities. The security architecture identifies seven security requirements that protect against all major security threats trying to attack the MANoN. These attacks are characterised by accidental or intentional generation, of either inside or outside origin, and using active or passive behaviour. The security architecture is defined based upon ITU-T Recommendations ***X.800, and X.805***.

This security architecture appears in our publication [75, 4].

Security Management for MANoN: A novel security-management system is proposed based upon Recommendation ITU-T M.3400 [58], which is used to evaluate, report on the behaviour of our MANoN and support the complex services our system might need to accomplish. In addition, we will concentrate on providing the essential components *Prevention* and *Detection*. Novel security mechanisms are used to satisfy the objectives of security requirements, such as *authentication, authorisation, availability, data confidentiality, data integrity and non-repudiation.* We assume that MANoN is operating in heterogeneous wireless environments such as WLANs and cellular systems.

In this novel mechanism, two different algorithms will be defined for two different scenarios.

- **ACM–MANoN:** The access control mechanism for MANoN proposes a prevention technique against malicious acts, which are provided using threshold cryptography digital certificates where all ad hoc networks are pre-defined and managed by other heterogeneous infrastructure-base. Moreover, a hierarchy trust model is used by the PKIs of the heterogeneous wireless networks, and provides a high level of security, availability and a well certification management service for MANoN. This mechanism is evaluated using the Network Simulator NS-2. NS-2 evaluation tests the proposed algorithm in a real network environment and measures communication costs using other evaluation metrics, such as *success ratio*, delay, average number of retries and overhead. The results of the evaluation study proves that ACM-MANoN is fully distributed security protocol that provide a high level of secure, available, scalable, flexible and efficient prevention management services for MANoN. ACM-MANoN appears in our publication [4].

- **BD-MANoN:** The behaviour detection mechanism for MANoN, propose a detection technique which may be used to differentiate between normal and malicious nodes. This detection algorithm is provided in a heterogeneous MANoN in which some of our networks are pre-defined and others are emerging surreptitiously. This mechanism will be carried out by our administrator nodes, which is based on the behaviour and actions of other nodes with comparison of our security policies. This mechanism is evaluated in a real time military environment, where different scenarios and policies have been introduced; this evaluation shows the availability, flexibility, and high level of security detection against malicious and untrustworthy nodes in the MANoN system. BD-MANoN appears in our publication [4].

1.4 Success Criteria

To judge the success criteria of our research, the following research questions must be fulfilled in our thesis:

- For a well deployed security architecture which has never been provided for MANoN, how can an end-to-end security architecture be applied to network entities, services and applications in order to detect and predict security vulnerabilities?
- Is the MANoN system securely managed? Security management includes three essential components: Security Administration, Prevention & Detection and Containment & Recovery, does the system contain any security solutions for these components?
- What kind of protection is needed and against what threats?
- What are the distinct types of network equipment and facility groupings that need to be protected?
- Providing authentication and authorisation will be major factor towards providing the other security requirements any system might need to present a secure system, the question is, does our research provide these requirements?

These criteria will be revisited in the conclusion chapter to argue that such solutions exist and met in our research.

1.5 Thesis Outline

The thesis is structured as follows:

Chapter 2 presents the characteristics and challenges of MANoN. It investigates the security issues in MANoN by discussing security requirements, security attacks and security challenges. It then provides the cryptographic background needed to illustrate previous work and the mechanisms proposed in this area of study and moreover, related work in the area of security management for MANoN.

Chapter 3 uses the two ITU-T Recommendations X.800 and X.805, to propose the security architecture for MANoN that provides the specification of a comprehensive, end-to-end security solution. The security architecture defines security requirements and how they could be applied throughout the MANoN system, taking into account the various security attacks it could face.

Chapter 4 examines the integration of heterogeneous wireless networks in order to enhance MANoN security. It proposes a novel security-management system based upon Recommendation ITU-T M.3400, which is used to evaluate and report on the behaviour of our MANoN and support complex services our system might need to accomplish. It assumes that a MANoN operates in a heterogeneous environment, and presents two algorithms for two different scenarios. The methodologies used to evaluate the two algorithms are illustrated.

Chapter 5 proposes a new security access control mechanism based on threshold cryptography digital certificates in our MANoN system, providing a set of security requirements: authentication, authorisation, data integrity, confidentiality, and non-repudiation. This is a fully distributed security protocol that provides a high level of secure, available, scalable, flexible and efficient security management services for MANoN. This mechanism is evaluated using the network simulator NS-2.

Chapter 6 proposes a novel security detection protocol for managing digital certificates based on behaviours in the MANoN system. This is a fully distributed security protocol that provides a high level of secure, available, scalable, flexible, reliable and efficient security management services for MANoN. This approach is validated using an attacks case study to cope with misbehaving nodes.

Chapter 7 the evaluation of our approach was made with a military case study holding two scenarios. The military case study proposed concerns defined and undefined mobile armies engaging in unknown high risk territory.

Chapter 8 summarises the work presented in this thesis, highlights the significance of the contributions made and discusses directions for future work.

Chapter 2

Overview on Mobile Ad hoc Network of Networks (MANoN)

Objectives

- Define basic security concepts
- Provide an overview for MANoN
- Present an overview of the network security
- Present an overview of the cryptography background

2.1 Mobile Ad hoc Network of Networks (MANoN)

Mobile Ad hoc Network of Networks (MANoN) is a group of large autonomous wireless nodes communicating on a peer-to-peer basis in a heterogeneous environment with no pre-defined infrastructure. In fact, each node by itself is an ad hoc network with its own management. MANoNs are evolvable systems, which mean each ad hoc network has the ability to perform separately under its own policies and management without affecting the main system; therefore, new ad hoc networks can emerge and disconnect from the MANoN without conflicting with the policies of others. The unique characteristics of MANoN make such networks highly vulnerable to security attacks compared with wired networks, or even normal mobile ad hoc networks. MANoNs are a combination of both ad hoc networks and network of networks; to elaborate more on MANoN we need to discuss each component separately. This chapter will consist of an overview of MANoN. The present research focuses on tackling the security challenges and proposing different security solutions for our MANoN. The following sections will investigate the security aspect of communication in MANoN by discussing the security requirements, security challenges, different security attacks, key management issues, and the mechanisms used in the literature to manage mobile ad hoc networks securely.

2.1.1 Mobile Ad hoc Network (MANET)

Mobile ad hoc networks (MANET) are increasingly popular and successful in the industry and commercial of wireless technology in the future, as indicated by the increasing use of Bluetooth. This section will focus on the unique characteristics of MANET and the most important challenges facing this type of network.

2.1.1.1 History and Background of MANET

The principle behind ad hoc networking is multi-hop (a scenario of multi-hop will be shown later) relaying, which traces its roots back to 500 B.C. Darius I (533-486 B.C.), the king of Persia, invented an innovative communication system that was used to send messages and news from his capital to the remote provinces of his empire by means of a line of shouting men positioned on tall structures or heights. This system was more than 23 times faster than normal messengers available at that time. The use of ad hoc voice communication was introduced in many ancient/ tribal societies with a string of repeaters of drums, trumpets or horns.

In 1970, DARPA (Defence Advanced Research Project Agency) [24] had a project known as Packet Radio, where several wireless terminals could communicate with one another on a battlefield. Packet radio extended the concept of packet switching (evolved from point-to-point communication networks) to the domain of broadcast radio networks.

During the 1970s, a group of researchers led by Norman Abramson (and others including N. Gaarder and N. Weldon) invented ALOHAnet [1], which linked the universities of the Hawaiian Islands together by broadcast property to send/ receive data packets in a single radio hop system. Even though ALOHAnet was established for fixed single-hop wireless networks, the ALOHA project led to the development of a *multi-hop* multiple-access packet radio network (PRNET) under the sponsorship of the Advanced Research Project Agency (ARPA) [2]. Unlike ALOHA, PRNET permits multi-hop communications over a wide geographical area, helping to establish the notion of ad hoc wireless networking in the same year [79].

2.1.1.2 MANET Characteristics

The study and development of infrastructureless wireless networks have been very popular in recent years. MANET belongs to the class of networks which does not require the support of wired access points or base stations for intercommunication. A mobile ad hoc network is unlike a static network, as it has no infrastructure. It is a collection of mobile nodes where communication is established in the absence of any fixed foundation. The only possible direct communication is between neighbouring nodes. Therefore, communication between remote nodes is based on multiple-hop. These nodes are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. Each mobile node acts as a host and a router, relaying information from one neighbour to another [94]. For example, in Figure 2.1, nodes *A* and *D* must enlist the aid of nodes *B* and *C* to relay packets between them in order to communicate.

MANETs have various defining characteristics that differentiate them from other wired and wireless networks, such as [110, 3, 76]:

- ***Infrastructureless***: MANETs are formed based on the collaboration between independent, peer-to-peer nodes that wish to communicate with each other for a particular purpose. No prior organisation or base station is defined and all devices have the same role in the network. In addition, there are no pre-set roles such as routers or gateways for the nodes participating in the network unless specific arrangements are provided.

- ***Dynamic Topology****:* MANET nodes are free to move around; thus they could be in and out of the network, constantly changing its links and topology. In addition, the links between nodes could be bi-directional or unidirectional.

- ***Low and Variable Bandwidth:*** Wireless links that connect the MANET nodes have much smaller bandwidth than those with wires, while the effects of interference, noise and congestion are more visible, causing the available bandwidth to vary with the surrounding conditions and to be even more reduced.

- ***Constrained Resources****:* In general, most of the MANET devices are small handheld devices ranging from laptops, smartphones and personal digital assistants (PDA) down to cell phones. These devices have limited power (battery operated), processing capabilities and storage capacity.

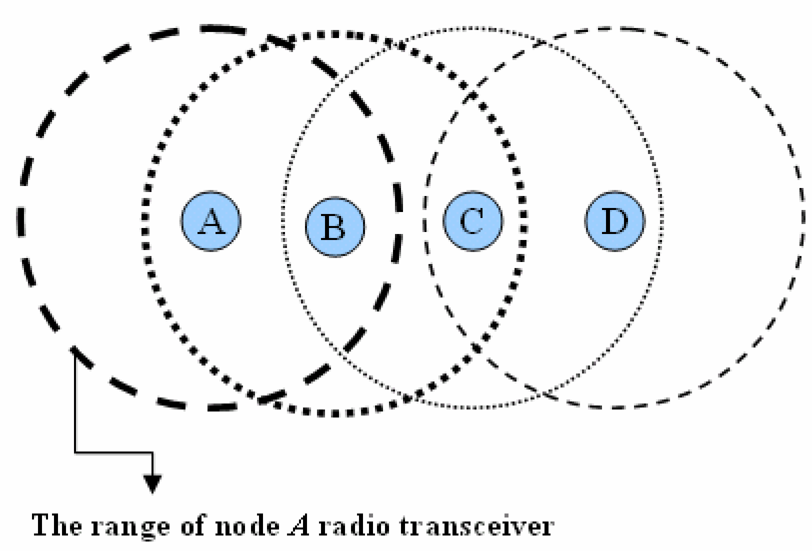


Figure 2.1: Mobile ad hoc network of four nodes, node A communicates with node D

- ***Limited Device Security:*** MANET devices are usually small and portable, and are therefore not restricted by location. As a result, these devices can be easily lost, damaged or stolen.

- ***Limited Physical Security:*** Wireless links make MANET more susceptible to physical layer attacks, such as eavesdropping, spoofing, jamming and Denial of Service (DoS). However, the decentralised nature of MANETs makes them better protected against single failure points.

- ***Short Range Connectivity:*** MANET depends on radio frequency (RF) or infrared (IR) technology for connectivity, both of which are generally short range. Therefore, the nodes that wish to communicate directly need to be in close proximity to each other. To overcome this limitation, multi-hop routing techniques are used through intermediate nodes that act as routers to connect distant nodes.

Since ad hoc networks can be deployed rapidly without the support of a fixed infrastructure, they can be used in situations where temporary network connectivity is needed. Examples include conferences, meetings, crowd control, shared whiteboard applications (office workgroup), multi-user games, robotic pets, home wireless networks, office wireless networks, search and rescue, disaster recovery and automated battlefields. These environments do not naturally have a central administration or infrastructure available.

2.1.1.3 MANET Challenges

The main challenges in the design and operation of MANET comes from the lack of a centralised entity (infrastructureless) - such as base stations, access points and servers, the possibility of rapid node movement and the fact that all communications are conducted over the wireless medium. Owing to the unique characteristics of wireless ad hoc networks, the major issues that affect the design, deployment and performance of an ad hoc wireless system and that are interesting research areas in MANETs are as follows:

- ***Medium Access Scheme:*** As ad hoc networks lack any centralised control, the distributed arbitration for the shared channel for transmission of packets is the primary responsibility of a medium access control (MAC) protocol [121, 63].

- ***Routing:*** The existence of mobility in ad hoc networks implies that links between nodes construct and break occasionally. Hence, new routing protocols are needed [69, 80].

- ***Multicasting:*** As ad hoc networks require point-to-multipoint and multipoint-to-multipoint voice and data communication, and as ad hoc networks are mobile, the nodes links need to reform periodically. Moreover, most of the multicast protocols rely on the fact that routers are static, and that once the multicast tree is formed, tree nodes will not move. However, this is not so for MANET [117].

- ***Energy Management***: As MANET nodes act as host and routers, and are powered by small batteries with limited lifetime, consequently, necessary consideration must be taken [68].

- ***TCP Performance:*** Unfortunately, Transmission Control Protocol (TCP) is unable to distinguish the presence of mobility and network congestion. Hence, some enhancement or changes are needed to ensure that the transport protocol performs properly without affecting the end-to-end communication throughput [39, 125].

- ***Service Location, Provision, and Access***: the question arises: should there be a continued assumption that the traditional client/Server RPC (Remote Procedure Call) paradigm is appropriate for MANET? Owing to the limitations in bandwidth and the heterogeneity of the devices in ad hoc networks, this may not be attractive. Also, how can a mobile device access a remote service in an ad hoc network or how it can advertise its desire to provide services to the rest of the devices in the network? All these issues demand research [126].

- ***Security***: The unique characteristics of MANET present a new set of serious and essential challenges to security design; these include open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These types of challenges clearly make a case for creating security solutions that achieve both broad protection and desirable network performance [22, 73, 126, 25].

Although MANETs are enjoying a growth in the number of applications and possess many attractive features, they nevertheless face several challenges, as is plainly shown above. Each of these challenges can be considered as a separate research area needing thorough examination.

2.2 Network Security

When discussing network security in general, three important aspects need to be considered: security requirements, security attacks and security mechanisms.

Security requirements include the functionality necessary to provide a secure networking environment, while security attacks cover the methods that could be employed to break these requirements. Security mechanisms are the fundamental structure blocks used to provide and enforce the security requirements.

2.2.1 Security Requirements

Security requirements will be a vital solution to different attacks and threats (explained in section 2.2.2). If the key requirements are provided, then security will be much easier to achieve. In addition, those security requirements listed below should be implemented in any system in order to provide a high level of security; however, implementing all those requirements in one system is impossible. Researchers have tried implementing a set of key requirements to provide major security needs to any system.

The key requirements are being defined by several unions such as the International Telecommunications Union represented by their ITU-T Recommendation X.805 and

X.800, and they are as follows [3, 76, 104, 32]: *Access control*; *Authentication*; *Non-repudiation*; *Data confidentiality*; *Data integrity*; *Availability* and *Privacy*.

Authentication: Authentication is essential to ensure that both end peers are who they claim to be (genuine) and not impersonators. Without proper authentication, no other requirement can be correctly implemented. For example, if two nodes are using symmetric-key encryption to exchange messages securely, and one of them becomes compromised as a result of the lack of proper authentication, then all encrypted material such as the shared key and the encryption algorithm will be readily available to that misbehaved node. Techniques to authenticate users securely are essential to the operation of MANET. Moreover, an adversary might masquerade nodes by gaining unauthorised access to resources and sensor information. Moreover, an adversary might interfere with the operation of other nodes in the network.

Authorisation and Access Control: This ensures that only authorised nodes have the permission and privilege to perform in the network. Nodes participating in the network need to have proper authorisation to access and share resources, services, applications and personal information on that network. There are various approaches to access control:

Discretionary Access Control (DAC) offers a means for defining the access control to the users themselves. Mandatory Access Control (MAC) involves centralised mechanisms to control access to objects with a formal authorisation policy. Role Based Access Control (RBAC) enforces the notion of roles within the subjects and objects.

Availability: Essential services must be provided by a node at any time when they are needed, irrespective of attacks. In addition, availability of a network means that its services should be accessible, when needed, even in the event of break-ins.

Data Confidentiality: This concerns preventing unauthorised entities (intermediate nodes) from understanding the contents of the message. Confidentiality is not restricted to survivability of users' information only, such as strategic or tactical military information, but also to the - survivability of the routing information. Confidentiality can be obtained using any of the well-known encryption methods with proper key management systems.

Data Integrity: Guarantee data is not modified, deleted, removed, recorded, corrupted and re-transmitted by unauthorised entities either by radio failure or malicious attack. This is most essential in circumstances such as banking, military operations and equipment controls (e.g. trains or planes) where such changes could cause serious damage.

Non-repudiation: This ensures that the receiver and sender can not deny receiving and sending packets to or from other nodes. This approach can detect and isolate the compromised node. If *A* received an erroneous message from *B* with the intention of breaking down *A*'s system, after that *A* can accuse *B* of providing proof of sending erroneous information, and expose *B* to other nodes to convince them that node *B* is a malicious node and not to route through *B* in the future. This is very important in cases of disagreement over some situations. This can be obtained using methods such as digital signatures that relate the data or action to the actual signer.

Privacy: Privacy ensures that the location and identity of nodes are protected against an adversary. Moreover, it provides protection of information flow so that an adversary can not gain information by observing it.

Other requirements the system might need [19]:

Timeliness: Routing updates should be delivered in a timely manner. Update messages that arrive late might reflect the wrong state of the network and might lead to a large loss in information.

Isolation: This requires that nodes should be able to identify misbehaving nodes and isolate them. Alternatively, routing protocols must be immune to malicious nodes.

Lightweight computation: Many devices connected to an ad hoc are assumed to be battery powered with limited computational ability. They might not be able to carry large cryptography algorithms.

Self-stabilisation: Nodes should be able to recover from attacks independently in real time without human intervention. If nodes are self-stabilising to malicious attacks, then the attacker will remain in the network, and continue sending erroneous messages in order to bring the system down, but it will be easier for nodes to locate the attacker.

Survivability: This is the capability of the system to fulfil its mission in a timely manner, in the presence of accidents, failures, intrusion or malicious attacks. Mission means restoring and maintaining essential services during and after the attack, even if a large portion of the system has been damaged or destroyed. Requirements of the survivability system are resistance to, recognition of, recover from, adoption and evaluation [89].

Anonymity: Neither the node nor the system should by default expose information, such as MAC address and IP address, that might put the system at risk.

2.2.2 Security Attacks

As mentioned, security in ad hoc wireless networks is very important, especially in military applications. The lack of any central administration makes MANET more vulnerable to attacks than wired networks. Consequently, attacks in ad hoc networks are generally divided into two broad categories, namely, *Passive* and *Active* attacks.

A passive attack refers to the attempts that are made by malicious nodes to perceive the nature of activities and to obtain information transacted in the network without disrupting the operation. For example, eavesdropping, active interference, leakage of secret information, data tempering, impersonation, message replay, message distortion and denial of service. Detection of passive attacks is complicated, since the network operation is not effected. Using encryption methods are great solution to overcome such problems example of encryption mechanisms is encrypting the data being transmitted, thereby making it hard for eavesdroppers to gain any active information from the data being transmitted.

An active attack refers to the attacks that attempt to alter, inject, delete or destroy the data being exchanged in the network. Those attacks can be executed by internal or external attackers, if the attacks are carried out by nodes that do not belong to the network (outside the network) that attack will be an *external attack*, which will be easier to defend, because users expect any act from an external node. Otherwise, if the attack comes from an insider node (part of the network), it will be an *internal attack*, which can cause considerable damage to the network because it is much harder to defend, as it is unfeasible to detect a malicious node and then prevent it from disrupting the network.

These attacks can be prevented by using regular security mechanisms such as encryption techniques and firewalls. Internal attacks come from compromised nodes that are actually part of the network; they are known as compromised nodes. Internal attacks are more serious and difficult to detect than external ones.

This section gives brief descriptions of some of the main active attacks known in most networks [3, 76, 32, 78, 31, 113].

- **Denial Of Service (DoS)**

  DoS is an active attack that attempts to make resources unavailable to its intended users. The attacker tries to prevent legitimate users to access services offered by the network. DoS can be carried out in different ways, but in the end causing the same problems. It can be carried out in the classical way by flooding centralised recourses (e.g. base stations) and permitting the system to crash or to interrupt its operation. Owing to the unique characteristics of ad hoc networks, DoS can be launched in different ways that do not exist in other wired or wireless networks and which can be launched at any layer of the protocol stack, for example, radio jamming and battery exhaustion on physical and MAC layers by disturbing the on-going transmissions at the wireless channels. On the network layer, an adversary could launch DoS on the routing protocols leading to a degrading in the QoS of the network by making routing protocols drop a certain number of packets. On higher layers, an adversary could bring down critical services, such as key management service (explained later).

- **Impersonation**

  The attacker tries to copy the behaviour or the action of an authorised node to gain the same facilities of the original node, either to make use of the network resources that might be unavailable to it under normal circumstances, or in an attempt to disturb network functionality by injecting erroneous routing information [45]. Man-in-the-middle attack is one form of impersonator. An adversary may read or falsify messages between legitimate users with out letting either of them know that they have been attacked.

- **Disclosure**

  A compromised node may try to disclose secret information to unauthorised nodes in the network; therefore communication must be protected against any eavesdropper trying to disclose confidential information that is being exchanged. Also, secret data must be protected from unauthorised access.

- **Repudiation**

  In simple terms, this occurs when nodes tries to deny having any involvement in particular action or communication with other nodes.

- **Routing Attacks**

  Those attacks occur on the network layer, when several types of attacks are mounted on the routing protocols which are aimed at disrupting the operation of the network. These are the major routing protocols attacks, which are described briefly:

  - **Routing table overflow:** The main goal of this attack is to create an overflow of the routing table and to prevent new legitimate routes from being created, which can be achieved by an adversary node trying to create routes to non-existence nodes.

  - **Location disclosure:** This type of attack can reveal some information about the location of the node or give a description of the network structure.

  - **Blackhole attack:** In this attack, a malicious node tries to advertise it self as having the shortest path to the specific destination (falsify advertisement) whose packets it wants to intercept. After gaining access between the required communications, the malicious node can do anything, like performing a DoS attack or alternatively it can use its place on the route as the first step in a man-in-the-middle attack.

- **Packet Replication:** In this attack, a malicious node replicates stale packets. This devours additional bandwidth and battery power resources available to the elements, and also causes unnecessary confusion in routing process.

- **Sleep deprivation:** This attack occurs in Ad hoc networks only because of the power limitation that ad hoc networks have. Thus, an attacker will try to consume battery life by requesting unnecessary routes or forwarding Packets (garbage) to nodes, by using for example Blackhole attack.

- **Military Attacks**

Every network used by the military will need full protection, by providing maximum security. In a military environment, routing attacks can be divided into two types:

-Strategic routing attacks: Strategic routing attacks include intelligence gathering. This type of attacks might cover desolation of enemy networks in the preparation of battle. Additionally, because of the attack, the attacker could gain some information about where the enemy is about to strike next. Nevertheless, once a routing attack has finished, the network can usually be brought back into use in a short amount of time.

-Tactical routing attacks: Tactical attacks could be used most effectively during battles. This attack could use the information gathered about the topology of the network. The main goal could be to disable some important part of a network temporarily by using DoS attacks.

- **Layers Attack**

  As seen in Figure 2.2, this section summarises the attacks that a MANET layer faces.

The security architecture for MANoN will be proposed in Chapter 3. It provides a comprehensive, end-to-end security solution for a MANoN in order to detect, predict, and correct security vulnerabilities. It identifies the security requirements, their objectives, and the means by which they could be applied to MANoN, taking into consideration the different security attacks it could face.

In order to enforce the implementation of the security requirements, a set of security mechanisms needs to be defined. Cryptography is one of the most powerful tools that can be used to achieve most of the security requirements, such as authentication, data confidentiality, data integrity and non-repudiation. The following section will provide the cryptographic background that is needed to understand the work already done to manage and secure a MANoN, as well as current research.

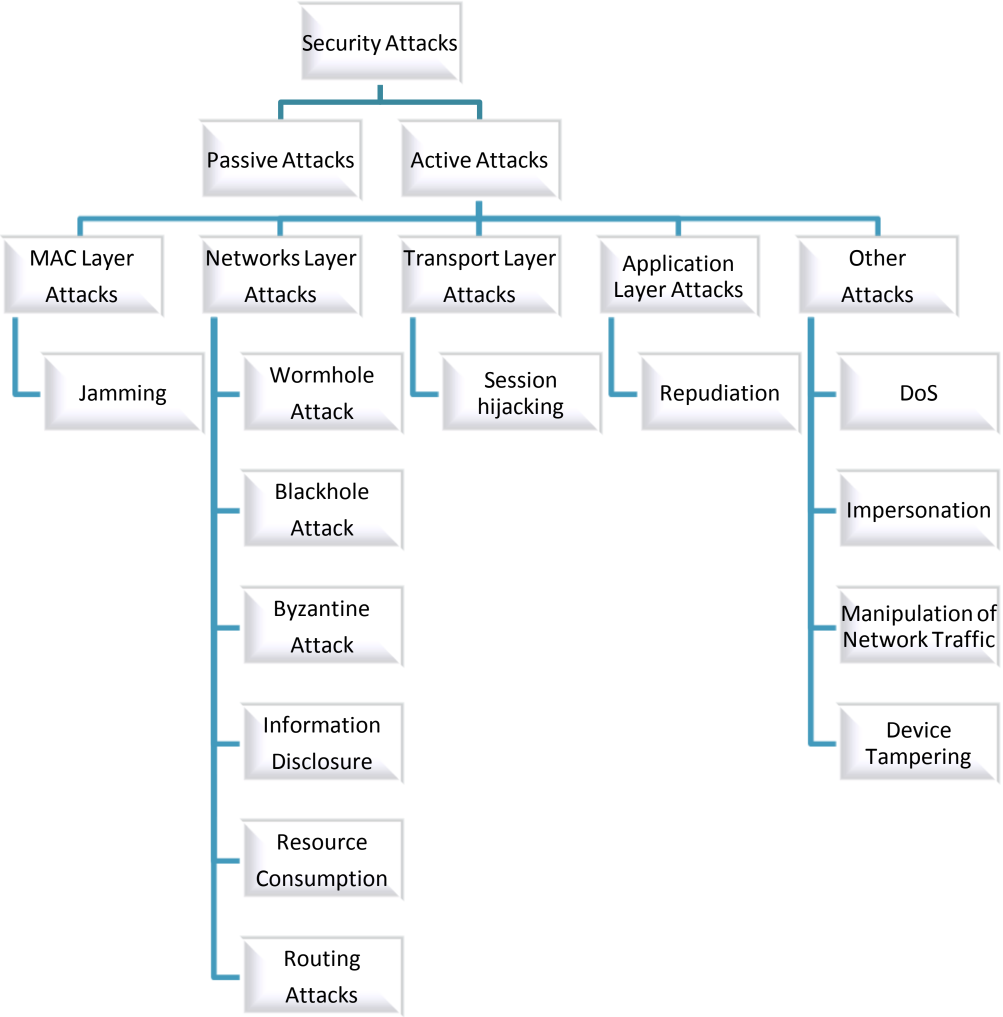


Figure 2.2: The Classification Security Layer Attacks [76]

2.2.3 Implementing the Security Solution for MANET

The proposed security architecture for MANoN is comprehensive and technology-independent. This section explains how this security architecture can be implemented.

There are various types of attacks against MANoN that have been dealt with in previous research. **Table 2.1** presents some of these attacks [96], [24], [46], [44], [122], [41, 17] and how they fit into the classifications defined in the security architecture (section 4.3), as well as mentioning some of the proposed methods of dealing with these types of attack.

Attack Name	Attack Type	Description	Proposed Solution
Eavesdropping	Passive Intentional (Internal or External)	Secretly gaining unauthorised access to confidential communications. It is easily carried out in many networking environments, especially in wireless networks.	Encryption, Intrusion detection schemes [41] [77]
Jamming	Active Intentional (Internal or External)	Adversary initially continually monitors the wireless medium in order to determine the frequency at which the receiver node is receiving signals from the sender. It then broadcasts signals on that frequency so that error-free reception at the receiver is hindered.	FHSS, DSSS [43]
Wormhole attack	Active Intentional (Internal or External)	Wireless transmissions are recorded at one location and replayed at another, creating a virtual link under attacker control.	Packet Leashes [42]
Blackhole attack	Active Intentional (Internal or External)	Discarding packets in a network based on some criterion. Attackers falsify advertises "good" paths (e.g. the shortest or more stable) to the destination node	SAR [122] [23]

		during the path-finding process (in on-demand routing protocols) or in the route update messages (in table-driven routing protocols)	
Byzantine attack	Active Intentional Internal	Attacks where adversaries have full control of a number of authenticated devices and behave arbitrarily to disrupt the network are referred to as Byzantine attacks.	[7] (Secure Routing Against Byzantine Failure)
Information disclosure	Active Intentional Internal	Compromised node may leak confidential or important information to unauthorised nodes in the network.	Secure Message Transmission (SMT) [85]
Resources consumption attack	Active Intentional (internal or External)	Attacker tries to consume/ waste away resources of other nodes present in the network by unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to nodes.	SEAD [46]
Sybil attack	Active Intentional External	A Sybil attack is one in which an attacker subverts the reputation system; it can be created by presenting multiple identities which can control a substantial portion of the system.	[27] Projecting FCAPS to Active Networks

Routing attacks	Active Intentional (Internal or External)	Several types of attacks mounted on the routing protocols which are aimed at disrupting the operation of the network, such as: routing table overflow, routing table poisoning, packet replication, route cache poisoning and rushing attacks.	ARAN [96][24] SEAD [46] ARIADNE [51]
Repudiation	Active International Internal	Refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication, regardless whether that communication is malicious or not.	ARAN [96]
Denial of service	Active Intentional Internal	Attacker aims to obstruct or limit access to a certain resource which could be a specific node or service or the whole network.	SEAD [46] ARIADNE [44]
Impersonation	Active Intentional External	Attacker uses the identity of another node to gain unauthorised access to resources or data. This attack is often used as a prerequisite to eavesdropping. By impersonating a legitimate node the attacker can try to gain access to the encryption key used to protect the transmitted data. Once this key is known by the attacker, he can	ARAN [24]

		successfully perform the eavesdropping attack.	

Table 2.1: Defence against MANoNs attacks

2.2.4 Cryptographic Background

Cryptography [103, 100] is the art and science of keeping messages secure from unauthorised persons; or it is the science of using mathematics to encrypt and decrypt data. Cryptography enables sensitive information to be stored or transmitted across insecure networks such as the internet so that it cannot be read by anyone except the intended recipient. The main goals of cryptography are confidentiality, integrity, authentication and non-repudiation.

In the idiom of cryptography, unique data sent from one user to another is called *plaintext*. This plaintext is converted into *ciphertext* by the process of *encryption* – that is, the application of certain algorithms or functions. An authentic recipient can decrypt/decode the *ciphertext* back into plaintext by the process of *decryption*. Mathematically, if M represents the plaintext message and C represents the ciphertext message, then we can say:

$$Encryption\ ::\ \mathrm{E(M)} = C$$

$$Decryption\ ::\ D(C) = M$$

The processes of encryption and decryption are governed by *keys*, which are small amounts of information used by the cryptographic algorithms. Keys must be kept secret to ensure security of the system, which is called a secret key. The secure administration of cryptographic keys is called *key management*.

There are two primary kinds of cryptographic algorithms: *symmetric key algorithms*, which use the same key for encryption and decryption, and *asymmetric key algorithms*, which use two different keys for encryption and decryption. In the following sections, these two algorithms will be discussed in addition to digital signature, digital certificate, Public Key Infrastructure (PKI) and Web of Trust (WoT) models.

2.2.4.1 Symmetric Key Algorithms

In conventional cryptography, symmetric key algorithms [103, 100] rely on the presence of the shared key at both the sender and receiver, which has been exchanged by some previous arrangement (e.g. through a secure communication channel). This shared key is used for both encryption and decryption. It means that symmetric key cryptography is the process whereby the sender and the receiver use the same key private key (k) to encrypt and decrypt. Symmetric encryption is illustrated in Figure 2.3. Alice encrypts the plain text message *m* using the shared key *k* and converts it into cipher text *c*. In order to recover the plain text message *m*, Bob decrypts the received cipher text *c* using the same key used for the encryption.

Symmetric-key algorithms can be divided into *stream ciphers* and *block ciphers*. Stream ciphers encrypt the bits of the message one at a time, while block ciphers take a number of bits and encrypt them as a single unit. Blocks of 64 bits have been commonly used; the Advanced Encryption Standard (AES) algorithm approved by National Institute of Standards and Technology (NIST) in December 2001 uses 128-bit blocks [81].

Symmetric key algorithms are usually quicker to execute electronically, but needs a secret key to be shared between the sender and receiver. When communication needs to be recognised among nodes, each one of the sender-receiver pair should share a key, which makes the system non-scalable. If the same key is used between more than two nodes, a breach of security at any one point makes the whole system vulnerable.

2.2.4.2 Asymmetric Key Algorithms

The problems of key management in symmetric key algorithms are solved by *public key cryptography* (*asymmetric key*) the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1976 [26]. Public key cryptography is forms of cryptography were a user has a pair of cryptographic keys - a *public key* and a *private key*. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

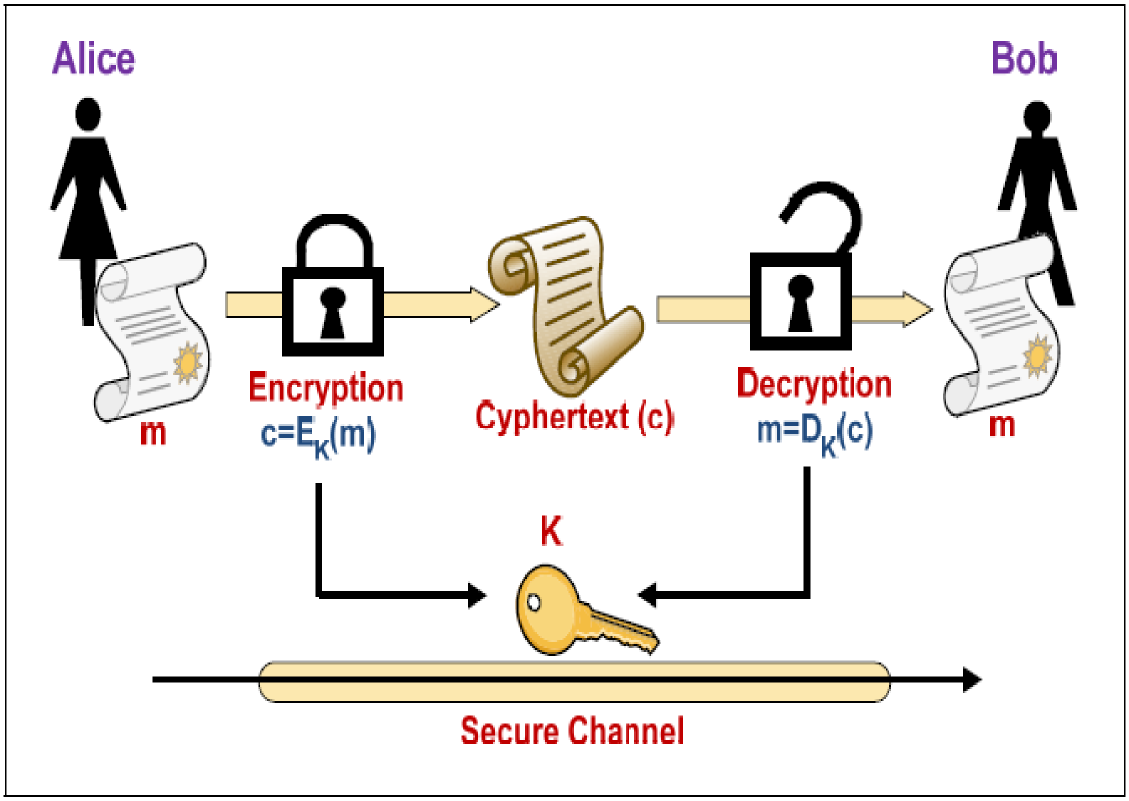


Figure 2.3: Symmetric encryption scheme [61]

The public key encryption scheme is illustrated in Figure 2.4. At the beginning, both Alice and Bob should have a pair of public and private keys. If Alice wants to send an encrypted message *m* to Bob, she first needs to get Bob's public key (PK_{Bob}) and make sure that this key is authenticated. This public key is used to encrypt the message *m* and convert it into cipher text *c*. Bob can then decrypts this cipher text using the corresponding private key (SK_{Bob}) which is known only by him.

The two main branches of public key cryptography are:

- **Public key encryption** — to ensure confidentiality a message should be encrypted with a recipient's public key which cannot be decrypted by anyone except the by the recipient possessing the corresponding private key.

- **Digital signatures** — to guarantee authenticity, integrity and non-repudiation a message signed with a sender's private key can be confirmed by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with.

A central problem for public-key cryptography is proving that a public key is authentic, and has not been tampered with or replaced by a malicious third party. The usual approach to this dilemma is to use a public-key infrastructure (PKI), in which one or more third parties, known as Certificate Authorities (CA), certify ownership of key pairs. Another approach, used by Pretty Good Privacy (PGP), is the Web of Trust (WoT) method to ensure authenticity of key pairs.

A very popular example of public key cryptography is the RSA system [103, 100] developed by Rivest, Shamir and Adleman, which is based on the integer factorisation problem. In RSA, to encrypt a message *m* or decrypt a cipher text *c*, the following calculations are performed:

$$c = m^e \; mod \;\; n$$

$$m = c^d \; mod \; n$$

A major benefit of public key cryptography is that it provides a method for employing digital signatures. Digital signatures permit the receiver of information to verify the authenticity of the information's origin, and also that the information is intact. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, meaning that it prevents the sender from arguing that he or she did not actually send the information.

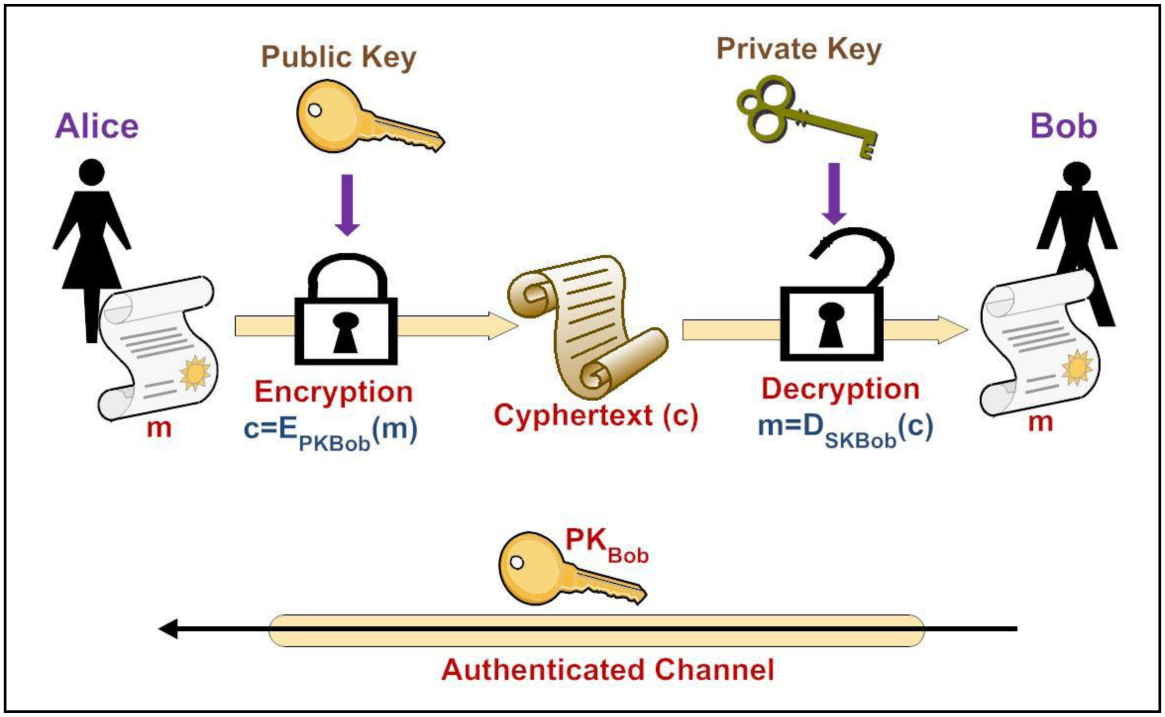


Figure 2.4: Asymmetric encryption scheme [103]

A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to imitate. It also attests to the contents of the information as well as the identity of the signer.

The basic manner in which digital signatures are created is illustrated in Figure 2.5. Instead of encrypting information using someone else's public key, it is encrypted with the sender's private key. If the information can be decrypted with the sender's public key, then it must have originated with that sender.

As can be seen in Figure 2.5, Alice wants to send a message *m* to Bob which is signed by her. Alice uses the hash digest of the message *m* and her private key to create the signature. First she uses a hash function on the message *m* and computes the hash digest. Then, she encrypts this digest using her private key (SK_{Alice}) and sends it with the message to Bob. Bob recomputed the digest by applying the same hash function on the received message *m* and compares it with the digest resulted from decrypting the signature using the public key of Alice (PK_{Alice}). If both digests match, then the message *m* must have originated from Alice and not been modified during transmission.

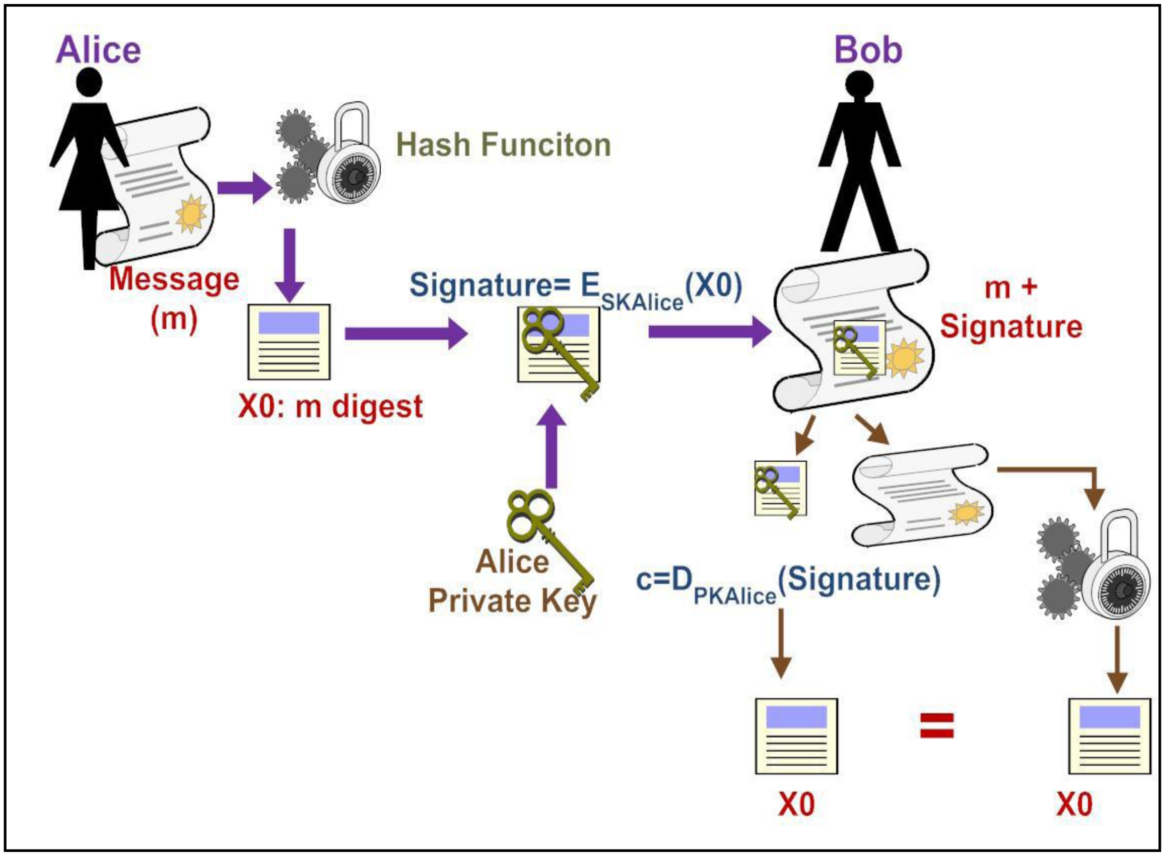


Figure 2.5: Digital Signature Example [100]

2.2.4.3 Digital Certificates

One issue with public cryptography is that users need to be sure that they are encrypting to the correct identity. In an environment where it is safe to exchange keys freely via public servers, *man-in-the-middle* attacks [32] are a potential threat. This type of attack is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages passing between the two victims.

For example, if Alice wants to send a message to Bob in a secure manner, she will ask for his public key. If Emma is able to intercept the messages between Alice and Bob and she is able to obtain the public key of Bob, the man-in-the-middle attack can be started. First, Emma will impersonate the identity of Bob and send her public key to Alice instead of Bob's public key. When Alice receives this key, she will believe that it really belongs to Bob and use it to encrypt the message and then send it back to Bob. This encrypted message is intercepted again by Emma.

This time Emma decrypts the message using her private key, keeps a copy of it and re-encrypts it using the correct public key of Bob. Once this message is received by Bob, he will believe that it was sent by Alice [114]. This example shows the need for Alice and Bob to have some way of ensuring that they are truly using each other's public keys rather than the public key of an attacker. Otherwise, such attacks would be generally possible, in principle, against any message sent using public-key technology.

Digital certificates are used to prevent the type of attack described above. A digital certificate is an electronic document which incorporates a digital signature to bind together a public key with an identity-information, such as the name of a person or an organisation and their address. The certificate can be used to verify that a public key belongs to an individual. In a typical *public key infrastructure* (PKI) scheme, the signature will be of a Trusted Third Party (TTP) called a Certificate Authority (CA). The signatures on a certificate are attestations by the certificate’s signer that the identity information and the public key belong together.

X.509 is a commonly used standard for clarifying digital certificates following the PKI scheme. It is published as ITU recommendation ITU-T X.509 [54]. The structure of a X.509, version 3, digital certificate is shown in Figure 2.6.

2.2.4.4 Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) contains the certificate storage facilities of a certificate server, but also provides certificate management facilities, and the ability to *issue*, *update*, *revoke*, *store*, *retrieve*, and *trust* certificates. The main feature of a PKI is the introduction of what is known as a Certification Authority (CA). A CA is an example of a TTP, which facilitates interactions between two parties who both trust the third party. A CA issues digital certificates for use by other parties.

A CA could be a person, group, department, company or other association that an organisation has authorised to issue certificates for its users. A CA's role is similar to that of a government’s Passport Office. A CA creates certificates and digitally signs them using the CA's private key. Because of its role in creating certificates, the CA is the central component of a PKI. Using the CA's public key, anyone wishing to verify a certificate's authenticity verifies the issuing CA's digital signature, and hence the integrity of the contents of the certificate and, most important, the public key and the identity of the certificate holder [121].

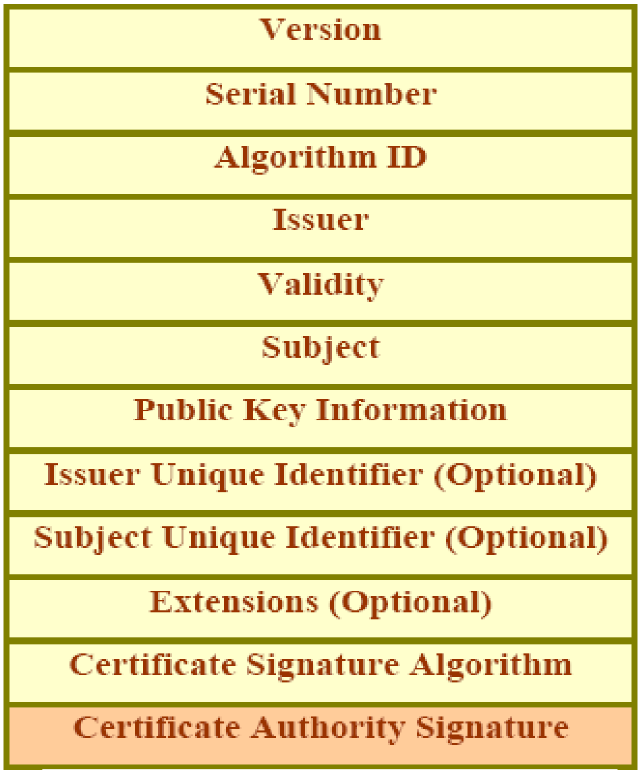
The main services provided by the PKI are [32, 54]:

- **Registration**: An important step before starting to issue a digital certificate for a user is to verify the identity of this user. This is the role of the Registration Authority (RA). The user will provide the RA with different information, such as name, e-mail address and organisation. The RA will then verify the correctness of this information by requiring the user to provide proof of identity such as a driving licence or ID-Card. Once the RA has proved the identity of the user, a certification request will be sent to the CA. RA in general is an optional part in the PKI. If it is not present, the registration service will become the responsibility of the CA.

- **Initialisation:** The most important information that a user needs to be initialised with before starting to use the digital certificate is the public key of the CA. The user will use the CA’s public key to verify any certificate signed by this CA.

- **Certification:** This is the main service provided by the PKI. After receiving a certification request from the RA, the CA will issue a digital certificate and then sign this certificate with its private key. The structure of the certificate should be defined; ITU-T recommendation X.509, for example standardised its certificates. All the information that needs to be completed in the certificate will be provided by the RA.

- **Key update:** The user’s keys and the corresponding digital certificate are valid for a specific time, varying from days to years. Therefore, this service is responsible for updating these keys on a regular basis, which depends on the application itself.



Version

Serial Number

Algorithm ID

Issuer

Validity

Subject

Public Key Information

Issuer Unique Identifier (Optional)

Subject Unique Identifier (Optional)

Extensions (Optional)

Certificate Signature Algorithm

Certificate Authority Signature

Figure 2.6: X.509 Digital certificate format

- **Revocation:** Each digital certificate has an issue and expiry date. Each certificate is revoked after its expiration time, as determined by the CA. Each CA should therefore update the certificates of its users before the expiry time. In addition to that, the CA needs to revoke a certificate if the private key becomes compromised or if any of the information included in the certificate has been changed.

- **Certificate and Revocation Notice Distribution**: After issuing a digital certificate, the CA should send this certificate to its owner who should be able to distribute the certificate to other users in the system. In the case of infrastructure-based networks, the digital certificates can be distributed through publicly accessible servers.

In addition to that, all the system users should be informed if any certificate has been revoked. A common method that can be used is called Certificate Revocation List (CRL). The CRL lists all the digital certificates that have been revoked. The CA will publish this CRL on a regular basis. The problem of the CRL is the time between compromising a certificate and revoking it. This time could be significant. This problem can be solved using online servers that allow the certificate users to query in real time the validity of any certificate.

2.2.4.5 Validity and Trust

Every user in a public key system is vulnerable to mistaking a fake certificate for a real one. *Validity* is confidence that a public key certificate belongs to its purported owner. It is essential in a public key environment where a particular certificate's authenticity must constantly be established. For example, in an organisation using PKI, no certificate is considered valid unless it has been signed by a CA which is trusted by everyone.
Validity can be established in various ways:

- **Manually**: the owner of a public key could be asked to hand over physically a copy of this key when it is required. This is often inconvenient and inefficient.

- **Certificate's fingerprint:** This is just like a human fingerprint. It is used by PGP [86, 127, 33], where every certificate has a unique fingerprint. The fingerprint is a hash of the user's certificate and appears as one of the certificate's properties. In PGP, this fingerprint can appear as a hexadecimal or a series of so-called biometric words, which are phonetically distinct and are used to make the fingerprint identification process a little easier. The verification of the latter fingerprint works only if the owner's voice is known.

- **Trust:** one way to establish validity of a certificate is to trust that a third party has gone through the process of validating it. A CA, for example, is responsible for ensuring that, prior to issuing to a certificate, he or she has carefully checked it to make sure that the public key really belongs to the supposed owner. Any user trusting the CA will automatically consider any certificates signed by the CA to be valid. In PGP [86, 127, 33], a CA can also be a *meta-introducer*. A meta-introducer gives not only validity to keys, but gives also the ability to trust keys upon others. The meta-introducer enables others to act as a *trusted introducer* who can validate keys with the same effect as that of the meta-introducer. They cannot, however, create new trusted introducers. In an X.509 [54] environment, the meta-introducer is called the *root Certification Authority* (root CA) and trusted introducers *subordinate Certification Authorities*.

In general, there are three different trust models that can be followed, which dictate how users will go about establishing certificate validity. The trust models are [86]:

- **Direct Trust**: It is the simplest trust model, which is used by most of the cryptosystems in some way. As can been seen in Figure 2.7, John trusts that Bob's key is valid because he knows where this key came from, and vice versa. An example of this model is the CA keys which are directly trusted by all users belong to the same PKI.

- **Hierarchical Trust:** This trust model is used by the PKI. There is a root CA which is directly trusted. This CA (*meta-introducer)* may certify certificates themselves, or may certify certificates that certify other certificates (*trusted introducer)* down some chain. As shown in Figure 2.8, the hierarchical trust model is represented as a tree. The leaf certificate's validity is verified by tracing backwards from its issuer to other issuers, until a directly trusted root (CA) certificate is found.

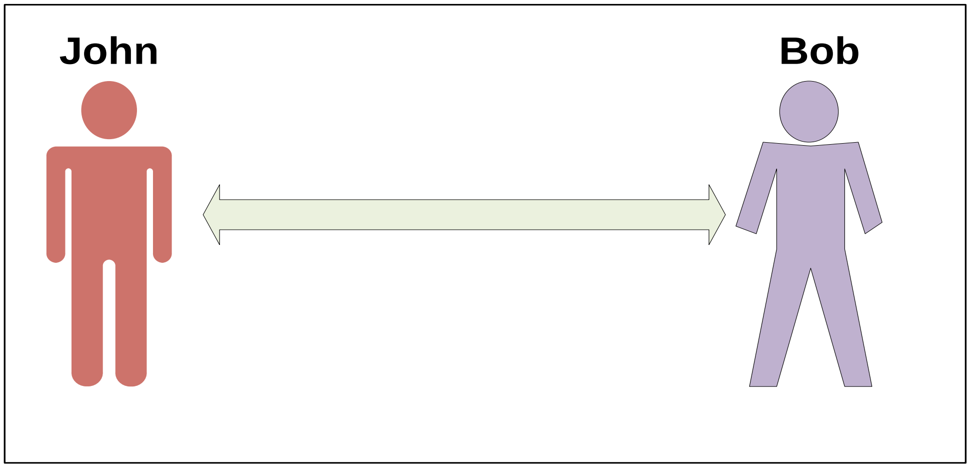


Figure 2.7: Direct trust model

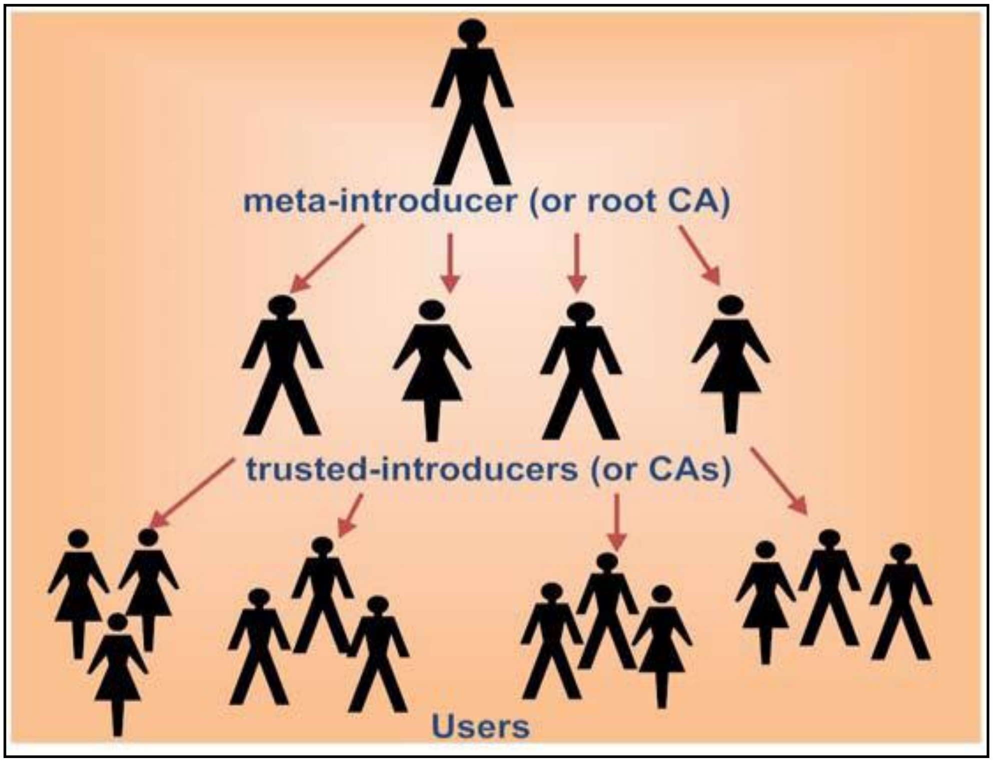


Figure 2.8: Hierarchical trust model

- **Web of Trust:** a web of trust uses both the direct and the hierarchical trust models. The certificate can be verified directly or by some chain going back to a directly verified certificate. PGP is a good example of using the web of trust model. PGP does not depend on any centralised CA. Any user could sign the certificate of another user. This process continues until a web of trust is established Figure 2.9.

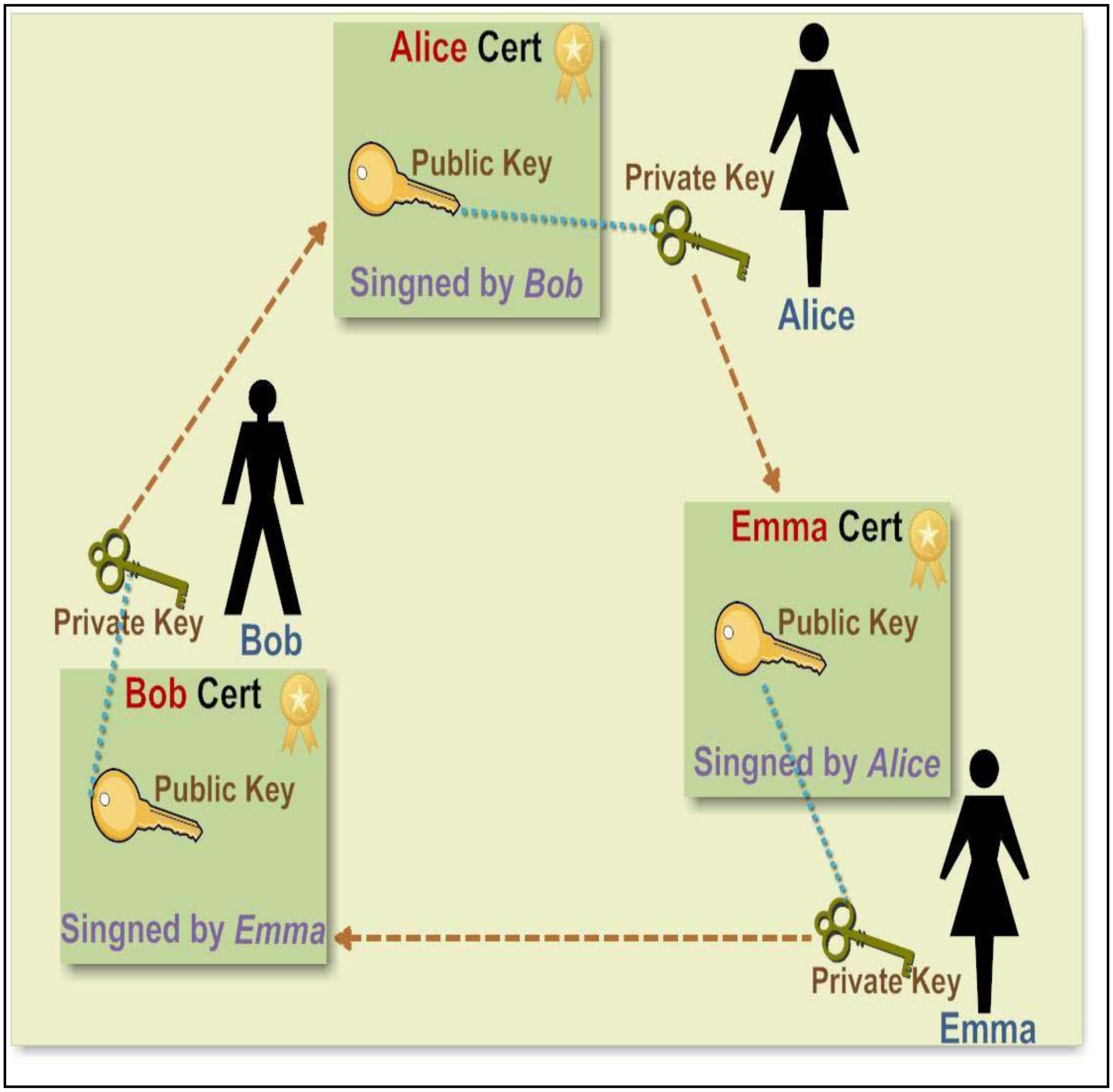


Figure 2.9: Web of trust model [100]

Understanding the possible form of attacks is always the first step towards developing good security solutions. Two types of security mechanisms can generally be applied: *Prevention* and *Detection*.

Prevention technique is always associated with cryptography; meanwhile, providing detection is much harder to achieve as it is used to discover an intruder attempting to penetrate the network to perform an attack.

2.3 Summary

In this chapter, the major issues and applications of Mobile Ad hoc Network of Networks were described. Moreover, this chapter discusses all the general information of ad hoc networks and tackles security challenges, security requirements and security attacks. The applications of ad hoc wireless networks include military applications, collaborative and distributed computing and emergency operations. Each of the challenges, security requirements and security attacks are discussed in detail.

In the next chapter, as we are dealing with security management for MANoN with concentration on prevention and detection techniques, we describe some of the solutions provided in the main features of our security management, showing appropriate key management services, a selection of intrusion detection techniques and best matching to our security management system.

Chapter 3

Review of Security Management for MANoN

Objectives

- Highlight MANoN challenges
- Present related work in key management service
- Present related work in IDS techniques
- Present related work in security management schemes for MANoN

3.1 Security Management for MANoN

This section discusses the issues and challenges in security management for MANoN. It also presents some solutions proposed in the literature to ensure MANoN security.

3.1.1 Network of Networks (NoN)

As mentioned, MANoN is a combination of both ad hoc networks and NoN, after highlighting the characteristics, challenges and background of ad hoc networks, NoN must be illustrated and fully described. First of all, the concept of NoN was recognised from system of systems (SoS), which are a collection of dedicated systems that attach resources and capabilities together to obtain new and more complex systems offering more flexibility then normal constant systems [10]. Following that, the new term NoN was presented; this is a number of networks interconnecting with each other by communication paths, and managed by a unified authority. Each network by itself is under its own legacy that enables it to function on its own; it comprises hardware and software, each potentially under separate management and ownership.

NoN provides new promising services to its users, in addition to the services provided by its component networks. The entities of a NoN are large autonomous, decentralised, mobile and dynamically configurable, all of which makes them capable of operating under partial information.

The concept of NoN is widely used in military and emergency situations; Spencer and Ironside [51] showed how the British army required this type of networks in their operations in order to reach a high level of security. As a result, we combined both ad hoc networks with NoN to create the new state-of-the-art Mobile Ad hoc Network of Networks (MANoN); although new advantages were obtained by creating this type of networks, new challenges have been noticed.

3.1.2 Security Challenges in MANoN

This section discusses certain unique characteristics of MANoN that make the design of a foolproof security management for MANoN a very challenging task. These unique characteristics can be summarised as follows [110, 76]:

- **Shared broadcast radio channel:** This is in opposition to wired networks, where a separate dedicated transmission line can be provided between two end users. The radio channel used for communication in MANoN is broadcast in nature, and is shared by all nodes in the network, allowing a malicious node easily to obtain data being transmitted

- **Insecure operational environment:** The operating environment where MANoNs are used may not always be secure. One example is a battlefield, where ad hoc nodes can move in and out of the enemy zone. Consequently, these nodes could become highly vulnerable to security attacks

- **Lack of central authority:** In wired networks and infrastructure-based wireless networks, monitoring the traffic on the network is possible through certain central points, such as routers, base stations, and access points, and to implement security mechanisms at such points. Since such central points are absent in MANoN, these mechanisms cannot therefore be applied in this type of networks

- **Lack of association:** MANoNs are dynamic in nature. Nodes can join and leave the network at any time. In addition, as each network is a legacy on its own, mobile networks can disconnect and evolve separately from the main MANoN. If there is no proper authentication mechanism that associates nodes with a network used, an intruder would be able to join the network easily and carry out attacks.

- **Limited resource availability:** The resources in MANoN, such as bandwidth, battery power and computational power are limited, making it difficult to implement complex cryptography-based security mechanisms in such networks.

- **Physical vulnerability:** In general, MANoN nodes are compact and hand-held in nature. They could easily be damaged and are also vulnerable to theft and to being lost.

- **Confliction of interest:** MANoNs consist of a number networks, each with its own management having the ability to operate and evolve separately from the main MANoN. Moreover, each network will have a set of policies to follow, regardless of the main MANoN; therefore, conflicts in policies might occur when moving from one MANET to another.

3.2 Key Management in MANoN

Most of the mechanisms used to provide security requirements mentioned in 2.2.1 need the use of some kind of cryptography keys. MANoN poses certain specific challenges in key management, owing to the lack of infrastructure in such networks. Three types of infrastructure that are absent in MANoN have been identified in [6]. The first type is routing infrastructure, in the form of fixed routers and stable links between them. The second is server infrastructure, consisting of online servers, which provide various services such as domain name service (DNS), directory services and trusted third party services.

The third type is organisational and administrative support, such as registration of users, issuing of certificates and cross-certification agreements between different user domains. Problems of applying cryptography, in order to achieve different security requirements in networks with full support infrastructure, are typically encountered; in MANoN, these problems present a real challenge. In fact, any cryptographic means is ineffective if key management is weak. Key management is a central aspect of security in MANoN, and requires the effective management of digital certificates.

Solutions to the problem of public key management in MANoN have already been proposed; they utilise one of two approaches; PKI or the web of trust. Our security mechanisms employ PKI-threshold cryptography; as a result, we will focus on PKI, as shown in the following sections.

3.2.1 PKI-based Key Management System

To adapt PKI to ad hoc networks, *threshold cryptography* is used to supply a distributed CA comprised of multiple mobile nodes that cooperatively provide certification services. The idea of the threshold scheme was introduced by Shamir in [98]. A *(k, n)* scheme allows a secret, for example a CA signing key to be divided into *n* shares, such that for a certain threshold $k<n$, any *k* components could merge and produce a valid signature; whereas fewer *k-1* shares would be unable to do so. The PKI-based solutions can be classified into *partially-distributed CAs* [126, 120, 4, 63, 68, 115], where some MANoN nodes are selected to play the role of CA, and *fully-distributed CA* [70, 71, 72], where all MANoN nodes can participate in playing the role of CA.

3.2.1.1 Partially Distributed Certificate Authority

The Partially-Distributed Threshold CA Scheme (Z-H) presented by Zhou and Haas [126] was one of the first efforts to address the key management issue in MANoN. The authors proposed a distributed public-key management service for ad hoc networks. The service as a whole has a public key *(PK)* and a private key *(SK).* It is assumed that the public key is known to all ad hoc nodes, while the private key is divided into *n* shares using an *(k, n)* threshold cryptography. These shares are assigned to *n* nodes called servers (Figure 3.1). To sign a certificate in this service, each server will use its share to generate a partial signature and then forward it to the combiner *c*. Having at least *k* correct partial signatures will allow the combiner to compute the complete signature.

When using a (2, 3) threshold cryptography scheme (Figure 3.2), in order to sign a message *m*, each server will generate a partial signature for the message *m* using its share, and then forward it to the combiner *c*. In this example, the server 2 fails to submit its partial signature even though, the system was able to generate the complete signature and attach it to the message *m*.

Besides threshold signatures, the proposed key management service also employs proactive share refreshing in order to tolerate mobile adversaries, and to adapt its configuration to changes in the network. Each server *i* generates randomly the following shares $(s_{i1}, s_{i2}..., s_{in})$ and then sends them to the other corresponding servers through secure channels. Once a server *j* receives all its shares from the other servers, the new share of *j* can be calculated using the formula: $s'_{j\,(new)} = s_{j\,(old)} + \sum_{i=1}^{n} s_{ij}$, as can be seen in Figure 3.3.

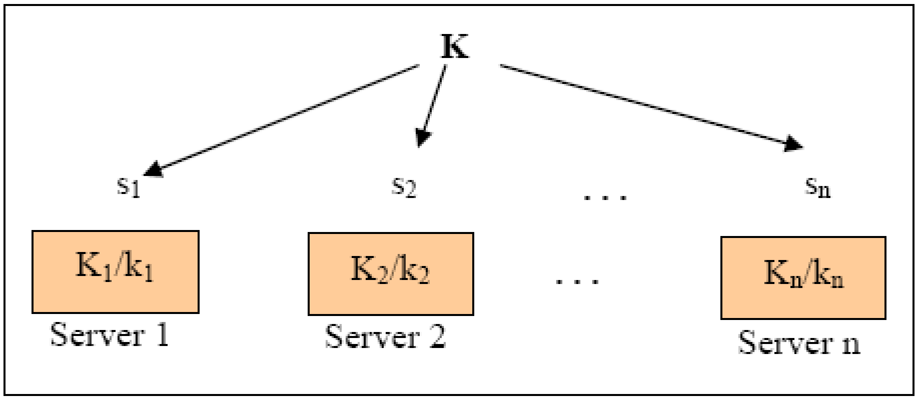


Figure 3.1: The configuration of (Z-H) Key Management Service

The application of threshold cryptography ensures that the system can tolerate a certain number $k-1 < n$ of compromised servers, in the sense that at least *k* partial signatures are needed to compute a correct signature. However, this proposal, assumes that there is an authority that initially empowers the servers, and that some of the nodes must behave as servers and others as combiners. Also, it does not describe how the value *k* is chosen, how a node can contact *k* servers securely and efficiently when the servers are scattered across the whole area, and how the server and combiner roles are distributed and used, or what the case would be if the node could not find enough servers or a combiner to generate the signature.

Nor is the question of the distribution of refreshed secret shares in an efficient and secure way addressed. In addition, this proposal has not been evaluated in real network environments in order to test the availability of the key management system, its communication costs and its ability to cope with different types of attacks. In Chapter 5, our Access Control Mechanism shows a dependency on this type of key management system, taking into consideration all the negatives the system might go through and trying to address them.

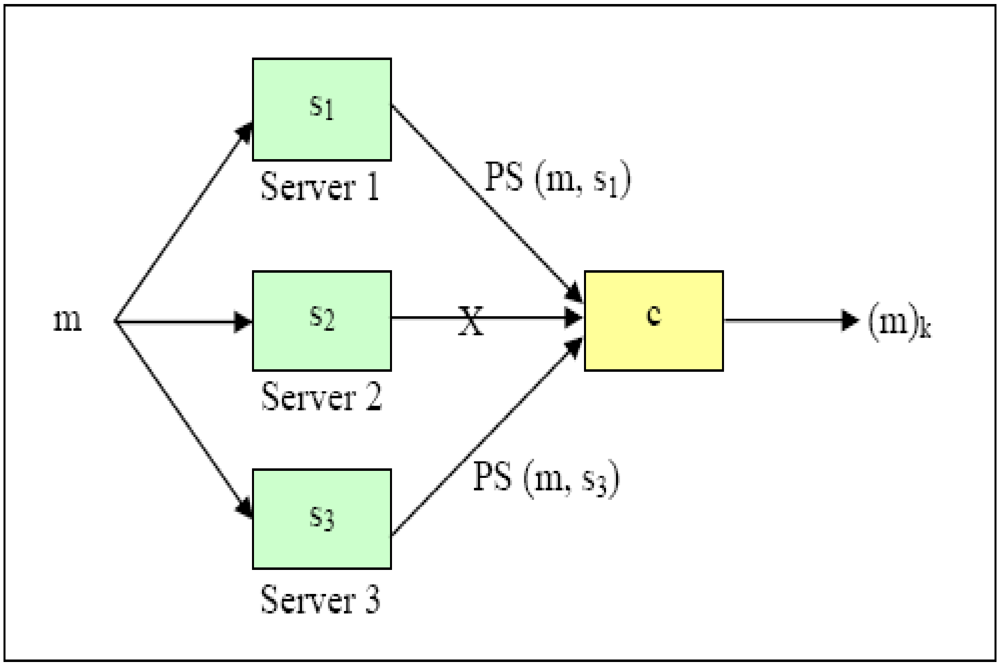


Figure 3.2: Threshold Signature

Mobile Certificate Authority (MOCA) is a key management system proposed by Yi, Naldurg, and Kravets [6, 120]. It is basically an extension of Z-H [126] that follows the same direction by building a distributed certificate service with the help of threshold cryptography. In their approach, the focus is on distributed CA services and communication between the nodes and the server nodes, which are called the mobile certificate authorities (MOCAs). MOCA suggests that the nodes exhibiting the best physical security and computational resources should be selected as MOCAs. The MOCA scheme also moves the combiner function of Z-H from the CA servers to the requesting end nodes. This improves the availability of the system, since the nodes no longer depend on the CA server nodes to combine the partial certificate signatures.

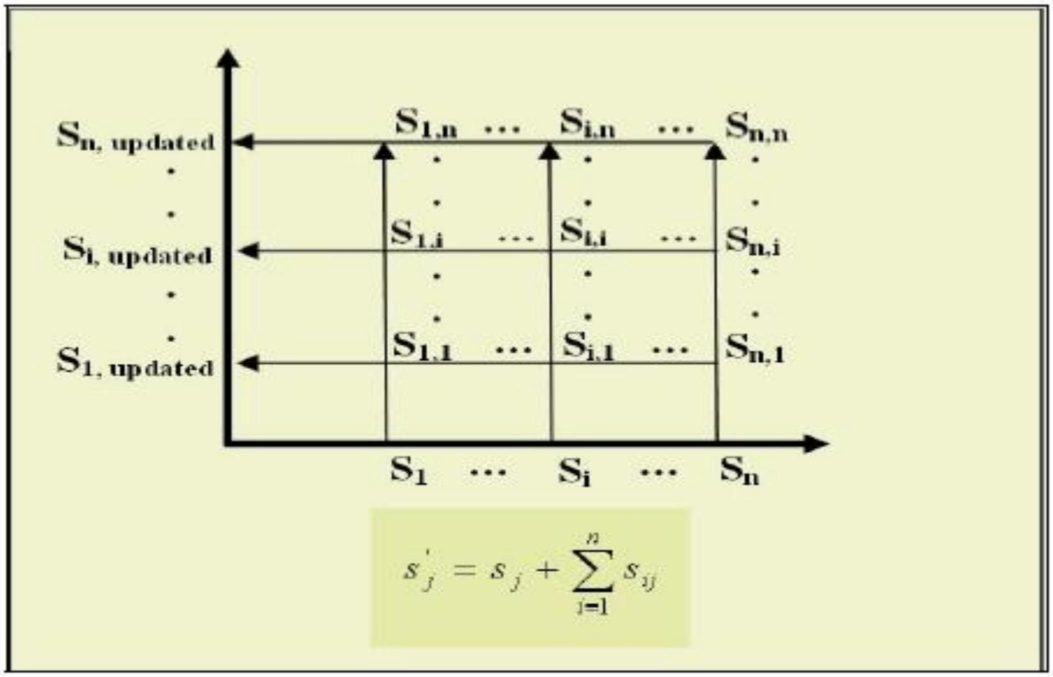

$S_{n,\ \text{updated}}$
$S_{i,\ \text{updated}}$
$S_{1,\ \text{updated}}$
$S_{1,n}$ ... $S_{i,n}$ ... $S_{n,n}$
$S_{1,i}$ ... $S_{i,i}$ ... $S_{n,i}$
$S_{1,1}$ ... $S_{i,1}$ ... $S_{n,1}$
S_1 ... S_i ... S_n
$s'_j = s_j + \sum_{i=1}^{n} s_{ij}$

Figure 3.3: Share refreshing

A MOCA certification protocol, MP, is proposed to provide efficient and effective communication between nodes and MOCAs. MP unicasts the certificate requests to β - specific MOCAs. Finding the path to these MOCAs is based on fresh routing entries or short distances. With the *(k, n)* threshold scheme, *k* MOCAs are required to complete a certification service. In order to increase the probability of receiving at least *k* responses, the value of β will be: $\beta = k + \alpha$ (selecting the value for the parameter α depends on the application itself). Once availability drops, the protocol returns to flooding (as in Z-H). MP maintains there own routing tables and co-exists with a standard ad hoc routing protocol.

MOCA leads to problems such as determining who judges the level of security and who chooses MOCAs, how to ensure that MOCAs are distributed uniformly and how nodes can discover the paths to MOCAs securely, since most secure routing protocols are based on the establishment of a key service. MOCA inherits high communication costs from threshold cryptography. Caching alleviates the problem to some extent when the network stays static, so that the cached routes are valid for a relatively long period of time. However, in the more volatile MANoN topology, this optimisation will be insufficient. Also, the MP maintaining its own routing tables in parallel with a standard ad hoc routing protocol is a waste of bandwidth, and as such is superfluous.

3.2.1.2 Fully Distributed Virtual CA

Ubiquitous and Robust Access Control (URSA) [70, 71, 72] provides a fully distributed threshold CA scheme. Similar to the partially distributed CA schemes H-Z and MOCA, it depends on a threshold signature system with a *(k, n)* secret sharing of the private CA key. As opposed to the partially distributed CA schemes, it provides a fairer distribution of the burden by allowing all nodes to get a share of the private CA key. A coalition of *k* one-hop neighbours forms the local CA functionality. It does not need any underlying routing protocol, only a node density of *k* or more one-hop neighbours. Mobility may help locate the required number of CA nodes. The nodes are trusted in the entire network when they receive a valid certificate. Any node holding a certificate can get a share of the private CA key. A new secret share is calculated by adding partial shares received from a combination of *k* neighbours. At the initial state of the system, a set of nodes will receive their certificates from a dealer. Once *k* nodes have been initialised, the dealer is removed. In this scheme, it is assumed that the certification service is delivered within one-hop neighbourhoods. The authentication of new nodes can be done through some reliable out-of-bound physical proof, such as human perception.

URSA takes the process a step further by letting every node hold a share of the CA secret key, and any *k* nodes are able to recover the key. However, as in the Z-H proposal

[126], the first *k* nodes must be initialised by a trusted authority. In addition to this drawback, the security depends on the system-wide parameter *k*. Since each node is now a certificate server, and compromising any *k* of them will disclose the private signing key, it actually endangers security to have a small *k* relative to the total number of nodes. However, if *k* is too big, it regresses to the basic form of threshold CA as Z-H. Limiting CA service requests to one-hop neighbourhoods is bandwidth-efficient and good for scalability. Distributing CA functionality boosts the availability of private key shares. Anyone capable of collecting *k* shares or more can reconstruct the private CA key. Like any public key format relying on a trusted entity, there is no easy way to change the private/public CA key pair during process. Finally, URSA seems to be susceptible to the *Sybil attack* [27]: an attacker can take as many identities as necessary to collect enough shares and restructure the system's private key.

3.3 Intrusion Detection Techniques

Intrusions are defined as any set of actions that compromise confidentiality, integrity and availability of the system. The intruder detection is the second line of defence which studies how to discover an intruder (internal or external node) attempting to penetrate the network to perform an attack [99]. The possible existing types of Intrusion Detection Systems (IDS) in MANoN are:

- **Standalone IDS**
    - no data exchanged; each node runs an IDS and detects attacks independently.

- **Distributed and Cooperative IDS**
    - every node participates in intrusion detection by having local and global detection decision-making.

- **Hierarchical IDS**
    - suitable for multilayered MANoN. Cluster head (CH) nodes in clusters perform the task of IDS and act as checkpoints such as routers in wired networks.

- **Mobile agent for IDS**
    - mobile agents are “codes” that can traverse the network. Each agent is assigned to perform a specific task (in this case IDS).

Many of IDSs have been proposed, most of them concentrate on cooperative analysis, yet not many methods are the same as our detection method; therefore, we concentrate on two types of intrusion detection systems (cooperative and mobile agents).

3.3.1 Intrusion Detection Techniques for Mobile Wireless Networks

Zhang, Lee and Huang [123] implemented local and collaborative decision-making in anomaly detection. In this approach, each ad hoc node participates in detecting locally and independently malicious acts. Each node holds an individual IDS agent that monitors local activities. It detects local traces and responds to them. If IDS detects an intrusion locally with strong evidence, then that node can decide that intrusion is happening and initiates an alarm response.

However, if the evidence is not strong enough but needs further investigation in a wider area in the network, then the IDS agent can start a collaborate procedure, which is a distributed consensus algorithm. This procedure works by generating the intrusion detection state information between neighbour nodes. The intrusion detection state information can vary from a simple level-of-confidence value such as:

- "with *P%* confidence, node A concludes from its local data that there is an intrusion";
- "with *P%* confidence, node A concludes from its local data and neighbour states that there is an intrusion";
- "with *P%* confidence, node A, B, C..., concludes from its local data that there is an intrusion";

to a more specific state that lists the suspects, like

- "with *P%* confidence, node A concludes from its local data that node X has been compromised";

Figure 3.4 shows the conceptual model of an IDS agent.

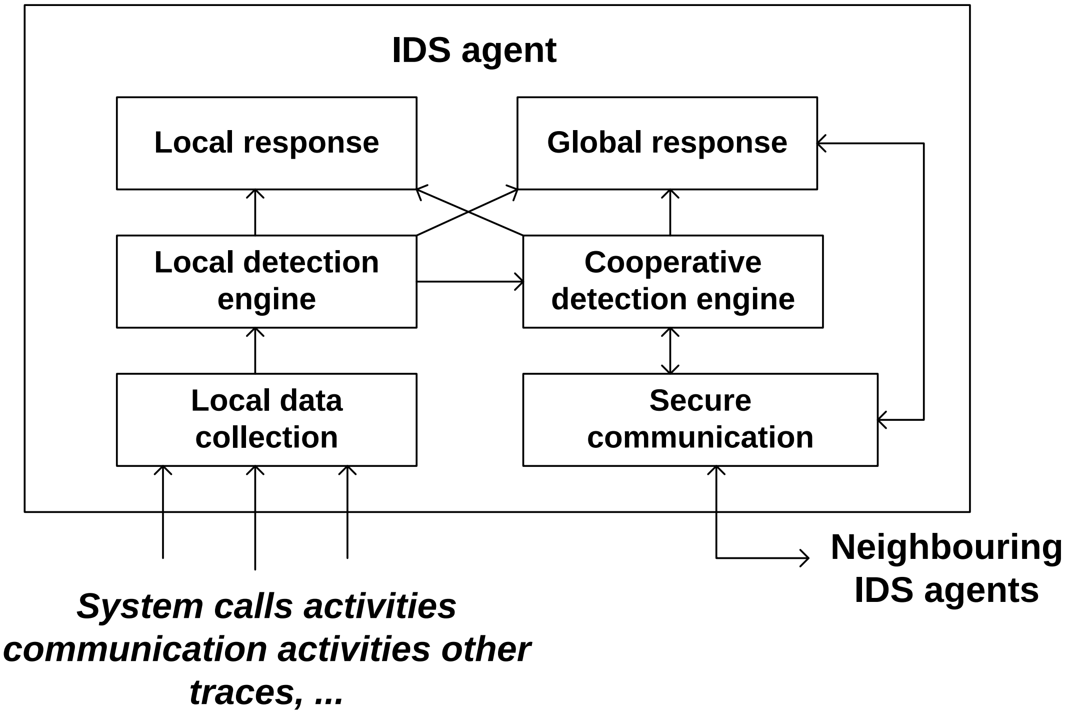


Figure 3.4: A conceptual model of an IDS agent

This architecture is well structured, yet the false alarm level of this algorithm is high; moreover, the authors mentioned collecting evidence without giving strong arguments of what type of evidence the agent is collecting and how it has been collected. There is no actual real-time analysis for observed nodes. Many situations might be changed depending on the environment, and there is no specific comparison with normal acts. Therefore, this algorithm is not sufficiently efficient for detection of malicious nodes in mobile ad hoc network systems.

3.3.2 Intrusion Detection Using Agents in Wireless Ad Hoc Networks

Kachirski, and Guha [64] proposed an IDS based on mobile agents technology; it provides a light weight and low-overhead mechanism based on the mobile security agent concept. Mobile agents are dynamic with high autonomy and mobility; they can automatically detect their current environment and respond accordingly. Moreover, tasks and works can be assigned to it by its users [20]. The main contribution of this approach is the efficient distribution of mobile agents with specific IDS tasks according to their functionality across the wireless ad hoc networks. Another advantage is providing a restricted computation-intensive analysis of overall network security to a few special nodes which are dynamically elected, and overall network security is not entirely dependent on any particular node.

The proposed IDS architecture shown in Figure 3.5 is built on a mobile agent structure that holds the specific functionality:

Network Monitor: Only certain nodes have sensor agents for network packet monitoring, since we are interested in preserving total computational power and the battery power of mobile hosts.

Host Monitoring: Every node on the mobile ad hoc network is observed internally by a host-monitoring agent. This includes monitoring system-level and application-level activities.

Decision Making: Every node decides on its intrusion threat level on a host-level basis. Certain nodes collect intrusion information and make collective decisions about network-level intrusions.

Action: Every node has an action module responsible for resolving intrusion situations on a host.

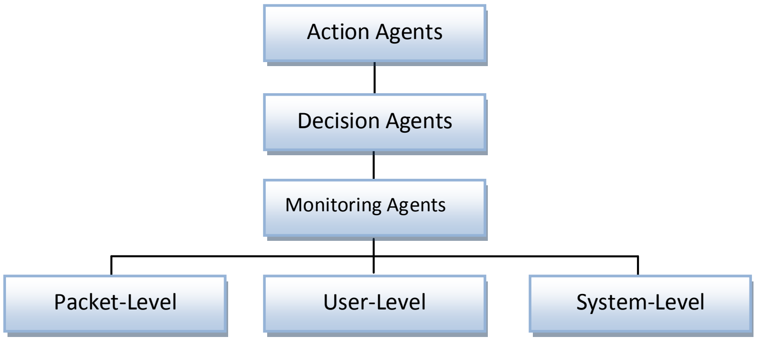


Figure 3.5: Layered Mobile Agent Architecture

This architecture provides hierarchical agents in order to represent a lightweight IDS with certain functionality, making the total network load smaller by separating the functional categories and assigning an agent to a specific function. In this way, the workload of a proposed IDS system is distributed among the nodes to minimise the power consumption and IDS related processing time by all nodes.

The author has provided an IDS based *decision making mechanism* and *Intrusion detection process* which assumes that each node with its Local Agent is responsible for evaluating other nodes with the help of other neighbour nodes to provide any kind of evidence. Those agents operate at both user and system level to detect suspicious activity. Although this algorithm looks convenient by reducing false alarms, it is unreasonable, because if an agent is itself compromised then the same problems of high false alarm and false reporting will occur. Also, if agents are compromised, the system might fail as the system depends on Cluster Head (CH).

3.4 Security Management Schemes

In general, different security schemes were used to deal with security management of MANET; none provides a full description of the three essential components of security management [59]. All research is focused on providing prevention or detection components. This subsection will highlight most of the schemes used to provide such management.

3.4.1 A Security Management Scheme Using a Novel Computational Reputation Model for Wireless and Mobile Ad hoc Networks

This type of security management is proposed by Azzedine Boukerche, and Yonglin Ren [112] and focuses on prevention technique, as it presents a set of management mechanisms based on trust and reputation to prevent malicious nodes from entering the trusted community.

This reputation management system depends on a central node with two assisted nodes evaluating those of its neighbour; it utilises a new technique named *Reputation Assistant Mechanism* (RAM), in which the central node has two reputation assistants, as shown in Figure 3.6.

Based on the evaluation of node C to the neighbour node D, a final decision will be taken for either excluding or to keeping node D in the community. To elaborate futher, Figure 3.6 shows that when node C tries to evaluate node D, it will inquire an assistant from its Reputation Assistant nodes A and B; therefore, these RA will provide node C with the trust value of node D. If neither of the RA nodes has the node D reputation in its community, it will respond with a VOID message.

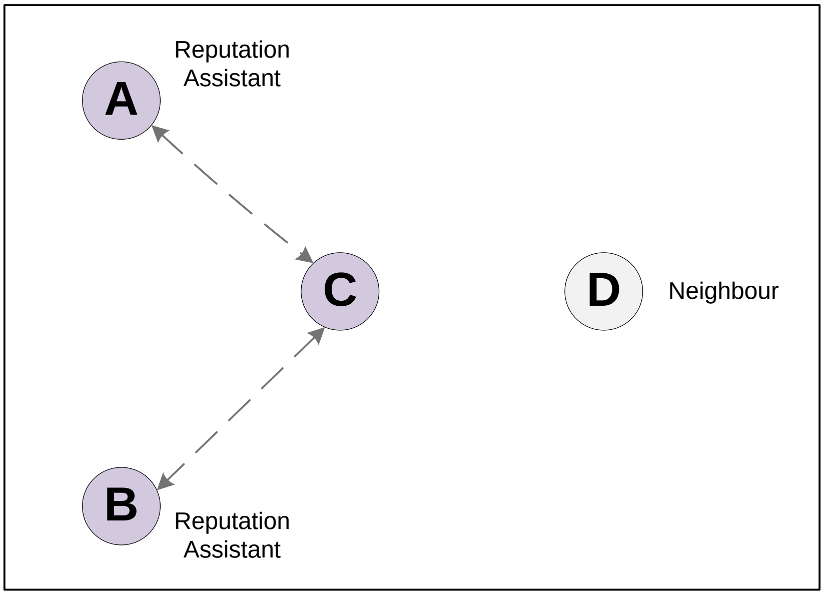


Figure 3.6: Reputation Assistant Mechanism

After receiving the trust values, node C measures the weighted means to make its final correspondent decision. The following formula calculates the average trust value *Trust* $_{AVG}$ from the set of reputation assistant *S*.

$$Trust_{\ AVG} = \frac{\sum_{i=1}^{n}\{Trust_{\ (RAi\ ,D)} \mid RAi\ \in S\}}{n} \quad (1)$$

Where $Trust_{(RAi,D)}$ is the trust value of the trust assistant RAi to a certain node D. Formula (2) computes the weight w_i of each reputation assistant, based on its own trust values in the entire set of reputation assistants S.

$$w_i = \frac{Trust_{\ (RAi\ ,D)}}{Trust_{\ AVG}} \qquad (2)$$

Formula (3) evaluates the node's final trust.

$$T = \frac{w_C \times Trust_{\ (C,D)} + \sum_{RAi\ \in S} w_i \times Trust_{\ (RAi\ ,D)}}{n+1} \qquad (3)$$

Where Trust$_{(C,\ D)}$ is the trust value of the central node C to the same node D and w$_c$ is 1 for the central node, because w$_c$ is taken as a standard to measure the importance of the reputation evaluations from other reputation assistance; therefore, node C will make the decision based on its and RA knowledge.

Discussion: first of all, trust and reputation is gaining more and more attentions; in ad hoc networks, nodes can gain or lose credit based on their behaviours, so only trusted nodes can participate in evaluating other neighbour nodes. This scheme divides the nodes into three parts, depending on their role in the community: the central node, reputation nodes and regular normal nodes.

The author did not mention to whom and how those roles have been assigned; moreover, depending on the neighbours' reputation, evaluation is inconsistent as different nodes might evaluate a specific action depending on specific acts and those acts are not compatible. For instance, if I trust and evaluate a person for fixing my car, do I trust him to fix my PC? So, from my point of view it is not efficient to use the trust and reputation scheme to prevent malicious nodes.

3.4.2 Security Management in Hierarchical Ad Hoc Network

Proposed in [29], this scheme suggests a security management policy based on the hierarchical routing; the key management system is managed in a hierarchical form, and each cluster head is a subserver. Actually, this scheme is based on the threshold cryptography cluster head which provides the key distribution to its nodes.

We found that this paper does not provide a real security management system nor secure policy system. The only improvement of this hierarchical security management system is a combination of cluster head and threshold cryptography key management services to solve the vulnerability of the CA.

3.4.3 Policy-Based Security Management for Ad Hoc Wireless Systems

Proposed in [5], this provides a policy-based network security management mechanism called the “Ripple Effect” to achieve integration and adaptation, and to activate different levels of security for ad hoc wireless systems. This mechanism has three distinguished functions:

Responsive Policy activation strategy – for protecting nodes under current attack; this type allows the host to raise the security policy level up to three levels, depending on the type of attack the system or the node is going through;

Pre-emptive policy activation strategy – for protecting nodes under potential attacks. In other words, when nodes are potentially under new attack, they send a warning message to their neighbours to prepare them against potential attacks;

Ripple-ring effect policy activation strategy – for controlling how to propagate attacking warnings for triggering different levels of defence techniques. Whenever an attack occurs in the network a certain level of host or network QoS degrades; therefore, this function helps to minimise these negatives.

Discussion: this scheme provides a well-defined policy-based security management system to provide prevention against malicious nodes trying to bring the system down. Few disadvantages have been shown in the system. First, many assumptions have been introduced; for example, the author assumes that all attacks are detectable. Second, as shown in Figure 3.7, the policy architecture is too complicated; i.e. it can be reduced to using fewer components with the same results.

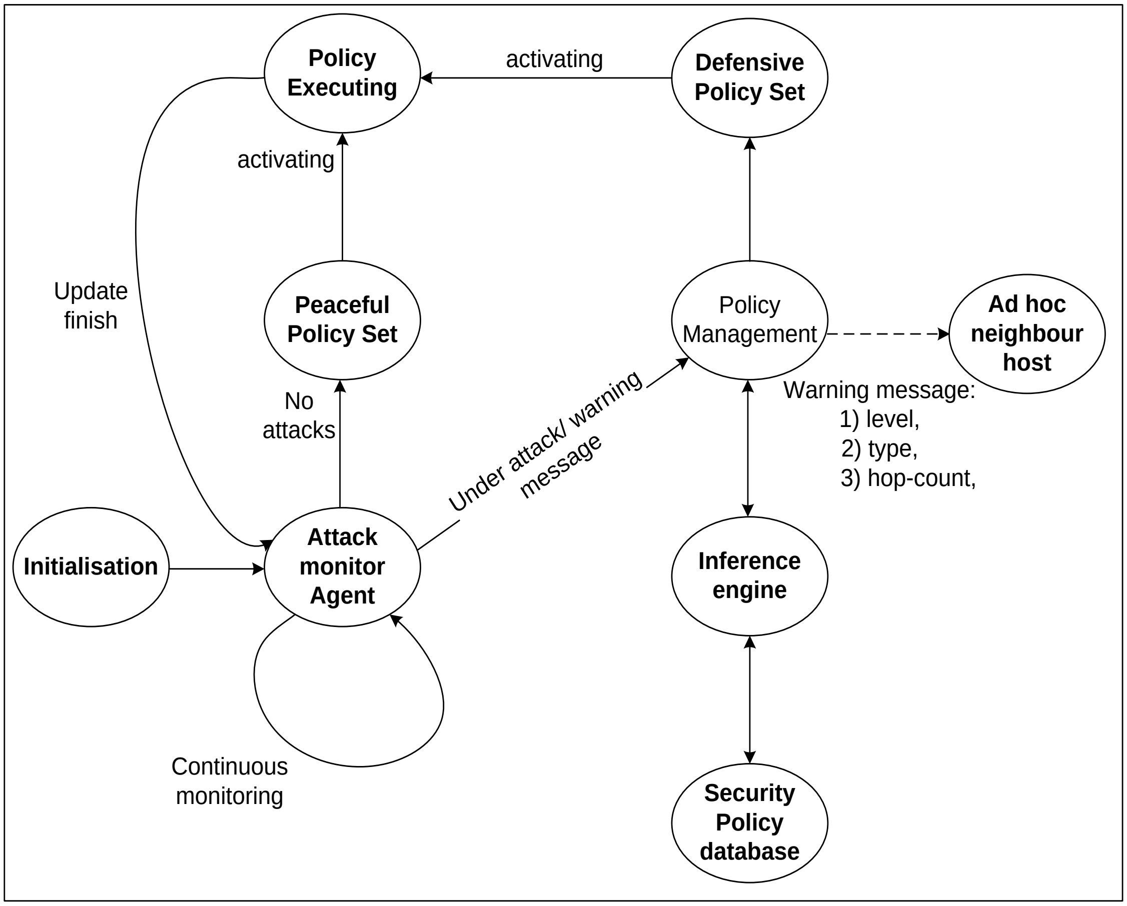


Figure 3.7: Responsive / Preemptive Security Management Architecture

3.5 Summary

This chapter has investigated the security issues in MANoN. It discussed previous work proposing to solve key management and security management with both essential prevention and detection services. For key management, efforts were made to adapt the hierarchical trust model in order to provide secure, available key management services, such as the MOCA and threshold cryptography. On the other hand, Intrusion Detection Systems using cooperative, individual and mobile agent have been introduced to provide an effective second line of defence against internal and external attacks, which are harder to predict. Finally, many security management systems, such as policy, hierarchical and reputation based schemes that implement the components prevention or detection security level of defence against malicious nodes have been discussed.

Solutions to the security problems in MANoN should be built upon a strong foundation. This means specialised security architecture for MANoN that helps in modelling this type of networks, addressing security challenges, defining security attacks and security requirements and describing principles and plans to achieve all the objectives of such requirements. Then a security mechanism must be proposed to enforce the implementation of these objectives. This methodology, by which MANoNs are to be secured, will be presented in the following chapters.

Chapter 4

Security Architecture for MANoN

Objectives

- Provide a novel end-to-end security architecture for MANoN
- Identify security requirements, layers, planes, their objectives and the means by which they could be applied to every part of the MANoN
- Address MANoN security challenges
- Propose a security solution for all wireless networks that satisfies MANoN requirements

4.1 Introduction

The unique characteristics of MANoN, such as broadcast radio channels, lack of central authority, lack of association, limited resources availability, physical vulnerability and policy conflicts (nodes following their own network policies and at the same time obeying different policies another MANET might enforce), which make such networks highly vulnerable to security attacks when compared with wired, infrastructure-based wireless networks and even normal ad hoc networks. This chapter proposes a technology-independent ***Security Architecture for MANoN*** based upon the ITU-T recommendations: X.800 [56] and X.805 [57]. This Security Architecture appears in our Publication [4] [75].

ITU-T X.805 defines a network security architecture created to address the global security challenges of service providers, enterprises, and consumers applicable to wireless, optical and wired-line voice networks. This security architecture addresses security concerns for the management, control, services and applications.

The proposed MANoN security architecture provides a comprehensive, end-to-end security solution for MANoN that could be applied to every wireless network that satisfies the MANoN requirements in order to predict, detect and correct security vulnerabilities any system might face. The Security Architecture identifies the security layers, security plans, security requirements, their objectives and the means by which they could be applied to every part of the MANoN, taking into consideration the different security attacks it might face.

This chapter is organised as follows: in section 4.2 the MANoN Security Architecture is proposed. This security architecture identifies the security requirements, security layers and security planes and proposes an end-to-end security solution for MANoN. Section 4.3 shows the security attacks the system might face. Section 4.4 shows the security solution in tabular form. Section 4.5 explains some technology-independent implementations for this Security Architecture. In Section 4.6, the conclusions will be drawn.

4.2 Security Architecture

As we have learned from the history of security attacks [19], security cannot be considered separately after the whole system has been designed; instead, security must be considered as an inseparable aspect in the development of the system. As a result, our security architecture was designed to address the global security challenges of consumers, users, services and other applications. In order to prevent any type of attacks, external or internal, passive or active, a set of requirements must be identified in our MANoN, as shown in Figure 4.1.

4.2.1 Security Requirements

Security requirements are a set of measures used to address a particular aspect of network security, which is governed by a specific set of security policies. The Security Architecture identifies seven major sets of requirements that protect the MANoN against all major security threats; these requirements are:

- *Authentication* means that the correct identity is known to the communicating parties. Nodes communicating with each other need to verify each other’s identity in order to be satisfied that they are communicating with the right party.

- *Authorisation* protects against unauthorised use of network resources. It ensures that only authorised nodes are able to perform in the network.

- *Availability* means that entities, services and resources are available against all kinds of attack. It ensures that there is no denial of authorised access to network services when needed, should unforeseen events impact upon the network.

- *Non-repudiation* means that entities cannot deny execution of a specific action. Any given entity should be liable for its actions, and should not be allowed to deny responsibilities of these actions. This is very important in cases of disputes or disagreement over some events.

- *Data Confidentiality* means that messages or packets are kept secure from any unauthorised disclosure. Data confidentiality ensures that the content of data’s cannot be understood by unauthorised entities. This can be achieved using any of the available encryption techniques provided, if proper access key systems are used.

- *Data Integrity* means that messages are unaltered during any communication. The data is protected against unauthorised modification, deletion, creation and replication.

- *Privacy* provides for the protection of information that might be gleaned from the observation of network activities. It implies protecting the identity and/or location of the node in the network. Protecting privacy involves more than data encryption, and requires more sophisticated techniques to hide the identity or the location of the user. This may be made possible by using mechanisms to hide routing topology.

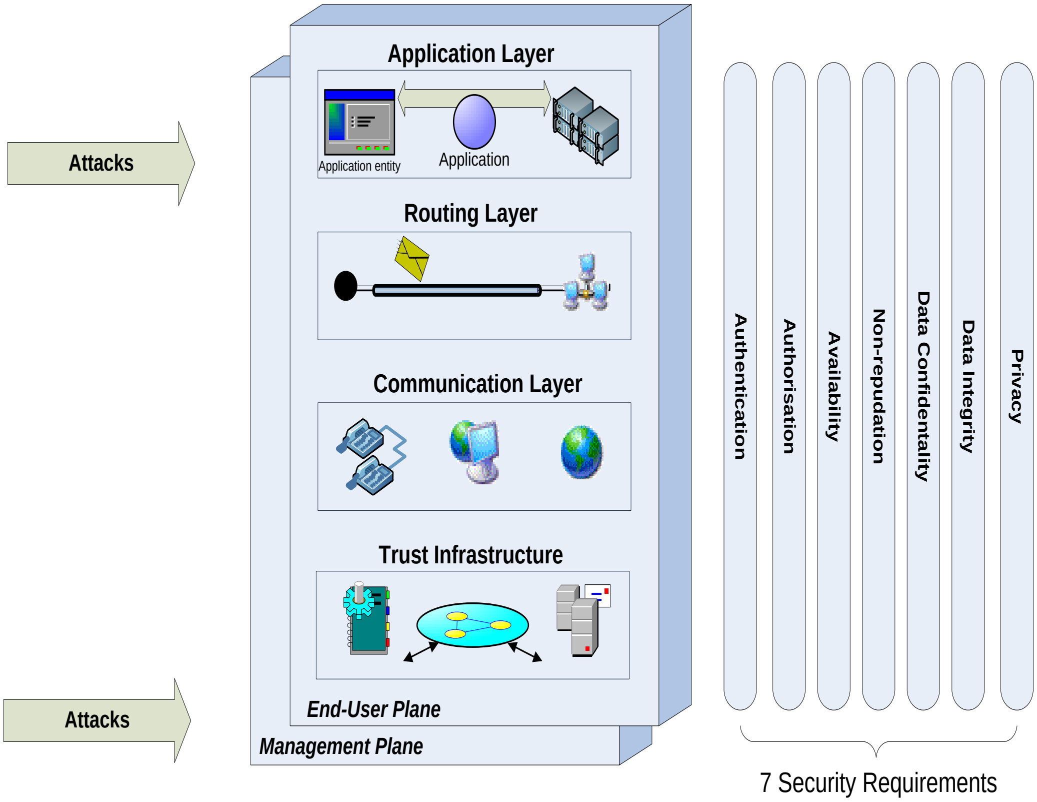


Figure 4.1: MANoN Security Architecture

After defining our security requirements, we must show how they can protect our system against all major security threats, and how they can be applied to every part of the MANoN. In order to provide a comprehensive, end-to-end security solution for MANoN, we need to satisfy these security requirements to a hierarchy of network equipment, which is referred to in our architecture as security layers.

4.2.2 Security Layers

In order to provide a comprehensive solution, we divide our complex MANoN logically into separate architectural components. This separation allows a systematic approach to the MANoN that can be used in the planning of new security solutions for other security threats our MANoN system might face.

Moreover, the success of the OSI [14] model applied in designing network protocols is a good example to follow in designing security protocols. A layered architecture can provide advantages such as modularity, simplicity, flexibility and standardisation of protocols. Figure 4.1 depicts four security architecture layers for MANoN, which are built upon one another to provide a network-based solution. The functionality of each layer is explained below.

- ***Trust Infrastructure*:** The trust infrastructure security layer represents a fundamental building block of the network, consisting of the basic relationships between nodes. An example is given by the explanation of Zhou and Hass [126] of a well-deployed PKI environment (threshold cryptography), as there is no centralised certification authority in which public and private keys are exchanged between all nodes. The security association established in the trust infrastructure layer must serve the upper layer security mechanisms.

- ***Communication***: The communication security layer consists of the transmission facilities protected by the security requirements, as well as security mechanisms such as physical protection mechanisms. Security Mechanisms deployed in this layer keeps transmitted data protected from eavesdropping, interception, alteration and dropping [52].

- ***Routing***: The routing security layer consists of basic transports and connectivity security mechanisms applied to routing protocols as well as the individual nodes; since each node in the ad hoc network acts as host and router, our MANoN is not different from that perspective. Moreover, nodes must exchange information about their neighbours to construct the network topology in order to apply one of the ad hoc routing protocols (Proactive, Reactive and Hybrid) [95]. Every node is required to participate in the routing activity, which makes routing an important aspect of our system in order to keep the network connected. Routing security layers involves two aspects: secure routing and secure data forwarding. In secure routing, nodes are required to cooperate in order to share correct routing information, thus keeping the network connected efficiently, whereas in secure data forwarding, data packets must be protected from tampering, dropping, and altering by any unauthorised party [88].

- ***Application***: The application security layer concentrates upon the security of the network-based services and network protocols that perform sub-network access operations from end-system to end-system, which are applied in our MANoN [118].

4.2.3 Security Planes

After dividing our security architecture into four layers, we need to handle it from different perspectives, so we consider two distinct security planes, the *Management Plane* and the *End-to-End User Plane*, which are protected by our security requirements from any threats and attacks, as shown in Figure 4.1.

- *Management Plane:* The management security plane supports FCAPS (Fault-management, Configuration, Accounting, Performance and Security) [12]. Moreover, it is concerned with the protection of OAM&P (Operation, Administration, Maintenance and Provisioning) [38], functions of the nodes, services and applications. This plane will highlight the management of our MANoNs system.

- *End-User Plane:* The end-user plane deals with end-user data flow (information flow) and security mechanisms related to the end users of the system [55].

These security planes are designed in such a way that events on one security plane are kept totally isolated from the other. At the same time, each layer depends on each other to provide a flexible foundation to our system and mechanism.

Having shown the components of our security architecture, we believe that each part has its own specific security needs. Hence by dividing it into layers and planes and by applying security requirements, we obtain a highly secure end-to-end security architecture.

4.3 Security Attacks

An attack is an assault on MANoN's security that attempts to evade security requirements and violate MANoN's security policies. Any system and network might be susceptible to attacks, causing the system to break down. MANoN attacks could be generated accidentally or intentionally, and could originate from inside or outside the network, resulting in an active or passive method of attack.

- **Accidental vs. Intentional.** An "accidental attack" has no premeditated intent. For example, network malfunctions and software bugs fall into this category. An "intentional attack" may range from informal examination using easily available monitoring tools to complicated attacks using special network knowledge.

- **Active vs. Passive.** An "active attack" attempts to alter network resources or affect their operation. A "passive attack" attempts to learn or make use of information from the network but does not affect network operations.

- **Insider vs. Outsider.** An "inside attack" (compromised node) is an attack initiated by an entity inside the security perimeter (an "insider"), i.e. an entity authorised to access network resources but using them in unauthorised way which is not approved by those who granted the authorisation. An "outside attack" is initiated from an unauthorised or illegitimate user of the network.

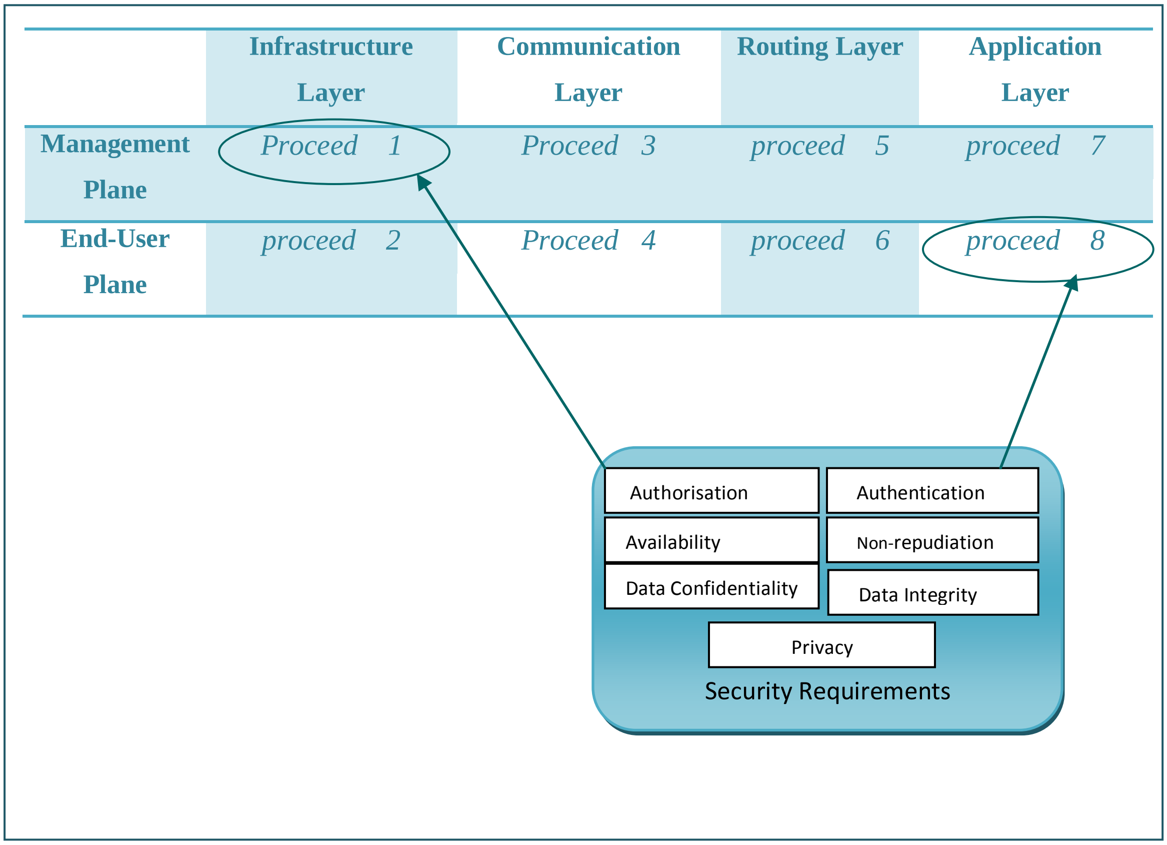
In the next section, a definition of a set of principles and a plan describing a security structure for the end-to-end security solution are given. The proposed solution identifies security issues that must be addressed in order to prevent these types of attack.

4.4 End-to-End Security Solution Designed in Tabular Form

Our security architecture proposes a comprehensive, end-to-end security solution for MANoN. This security solution addresses the global security challenges of MANoN in order to predict and correct security vulnerabilities.

Figure 4.2 presents the security architecture in tabular form, showing the interaction of the eight proceeds between the security layers and security planes.

Each of the eight proceeds represents a unique perspective for consideration of the seven security requirements. It should be noted that the satisfaction of the security requirements will raise different definitions and objectives, and will consequently comprise different sets of security measures. The tabular form is a conventional method of describing the aims of the security requirements for each proceed. Therefore, Tables (1) to (8) describe the objectives of the security requirements for the eight proceeds.



	Infrastructure Layer	Communication Layer	Routing Layer	Application Layer
Management Plane	*Proceed 1*	*Proceed 3*	*proceed 5*	*proceed 7*
End-User Plane	*proceed 2*	*Proceed 4*	*proceed 6*	*proceed 8*

Figure 4.2: Security solutions in tabular form

Securing the management plane of the Trust Infrastructure layer is concerned with securing the operations, administration, maintenance, and provisioning (OAM&P) of the high priority nodes (Servers and Combiners) in the MANoN system. **Table 4.1** explains the objectives fulfilled by applying the security requirements to the infrastructure layer in the management plane.

<table>
<tr><th colspan="2">Proceed 1: Infrastructure Layer & Management Plane</th></tr>
<tr><th>Security REQ.</th><th>Security Objectives</th></tr>
<tr><td>Authorisation</td><td>Ensures only authorised nodes can gain access to different MANETs. Ensures that only high priority nodes can perform administrator or management activities on other nodes or network devices. This applies to all MANoN management nodes.</td></tr>
<tr><td>Authentication</td><td>Ensures that the identities of the performing administrator or management activities on nodes or network devices are who they claim to be in each MANET.</td></tr>
<tr><td>Availability</td><td>Ensures the availability of high priority nodes and services provided by them. This includes protection against all active attacks (DoS) and passive attacks (eavesdropping) of the administrative authentication information.</td></tr>
<tr><td>Non-repudiation</td><td>Provides a record identifying the nodes performing administrative or management activity on the nodes or network devices and the action that was performed. This record can be used as evidence of the originator of the administrative or management activity.</td></tr>
<tr><td>Data Confidentiality</td><td>Ensure that data transferred between the administrative entities cannot be viewed or understood (e.g. keys and data bases). Protects the administrative authentication information (e.g. administrator identification and passwords) from unauthorized access or viewing.</td></tr>
</table>

Data Integrity	Ensures that the data transferred between the administrator nodes are not modified, deleted, created or replicated.
Privacy	Protects the information that can be used to identify high priority nodes and their network devices, base station location and identity from unauthorised nodes.

Table 4.1: Applying security requirements to the Infrastructure Layer, Management Plane

Securing the end-user plane of the infrastructure layer is concerned with securing user-data and voice as it resides in each high priority node in the system. **Table 4.2** shows the objectives of applying the security requirements to the Infrastructure layer at the management plane.

Proceed 2: Infrastructure Layer & End-User Plane	
Security REQ.	**Security Objectives**
Authorisation	Ensures that only high priority authorised nodes can gain access to different end-user data of each MANET.
Authentication	Identifies the identities of the high priority nodes attempting to gain access to end-users data in every MANET.
Availability	Ensures the availability of all end-user nodes and services provided (e.g. providing credentials) by them. This includes protection against all active attacks and passive attacks of the administrative authentication information.
Non-repudiation	Provides a record identifying the node performing activity on the end-user nodes that is actually performed. This record can be used as evidence of the access to end-user data.
Data Confidentiality	Ensures that data transferred between the end-users cannot be viewed or understood. Protects the end-user information from unauthorized access or viewing.

Data Integrity	Ensures that the data transferred between the end-user and the high priority nodes are not modified, deleted, created or replicated.
Privacy	Protects the information that can be used to identify end-user nodes and their network devices, base station location and identity from unauthorised nodes.

Table 4.2: Applying security requirements to the Infrastructure Layer, End-user Plane

Securing the management plane of the communication layer is concerned with securing the operations, administration, maintenance, and provisioning (OAM&P) of the network transmission facilities. **Table 4.3** shows the objectives of applying the security requirements to the communication layer in the management plane.

Proceed 3: Communication Layer, Management Plane	
Security REQ.	Security Objectives
Authorisation	Ensures that only authorised nodes are allowed to perform administrator or management activities of network transmission facilities.
Authentication	Verifies the identity of the nodes that are performing administrator or management activities of the network transmission facilities.
Availability	Ensures the availability of the transmission facilities and services provided by the high priority nodes. This includes protection against all active attacks and passive attacks of the administrative authentication information.
Non-repudiation	Provides a record identifying the entities or devices performing the administrative or management activity of the network transmission facilities and the action that was performed. This record will be used as proof that the administrative or management activity was performed with an indication of the nodes or network devices that

	performed it.
Data Confidentiality	Protects all files used in creation and execution of the network transmission facilities from unauthorised access or viewing. This applies to files stored or being transmitted across the network. Protects the network transmission facilities' administrative or management information (e.g. user identification and passwords, administrator identification and passwords) from unauthorised access or viewing.
Data Integrity	Ensures that all files used in the creation and execution of transmission facilities can not be modified, deleted, created or replicated. This protection applies to files inhabitant in nodes and network devices being transmitted across the network or stored as offline. The same type of consideration is applied to transmission facilities administrative or management information (e.g. administrator identification and passwords, user identification and passwords).
Privacy	Protects the information that can be used to identify transmission facilities' administrative or management systems from unauthorised entities.

Table 4.3: Applying security requirements to the Communication Layer, Management Plane

Securing the end-user plane of the communication layer is concerned with securing the user-data and voice of the network transmission facilities. **Table 4.4** shows the objectives of applying the security requirements to the communication layer at the end-user plane.

Proceed 4: Communication Layer & End-User Plane	
Security REQ.	Security Objectives
Authorisation	Ensures that only authorised nodes can gain access to different end-user data of each MANET for all transmission facilities.
Authentication	Identifies the identities of the nodes to communicate or access end-users' data in every MANET.
Availability	Ensures the availability of all end-user transmission facilities and services provided (e.g. providing credentials) by them. This includes protection against all active attacks and passive attacks.
Non-repudiation	Provides a record identifying the node performing activity on the end-user nodes and the action that is actually performed. This record can be used as proof of the access to end-user data.
Data Confidentiality	Ensures that data transferred between the end-users cannot be viewed or understood. Protects the end-user information from unauthorized access or viewing.
Data Integrity	Ensures that the data transferred between the end-user nodes are not modified, deleted, created or replicated. This applies to the configuration information resident in nodes and network devices, being transmitted across the network or stored offline.
Privacy	Protects the information that can be used to identify transmission facilities of the end-user nodes, base station location and identity from unauthorised nodes.

Table 4.4: Applying security requirements to the Communication Layer, End-user Plane

Securing the management plane of the routing layer is concerned with securing the operations, administration, maintenance and provisioning (OAM&P) of the transmitted nodes. **Table 4.5** shows the objectives of applying the security requirements to the routing layer in the management plane.

Proceed 5: Routing Layer, Management Plane

Security REQ.	Security Objectives
Authorisation	Ensures that only high priority nodes are authorised to perform administrator or management activities on transmitted nodes.
Authentication	Verifies the identity of the high priority nodes that is performing administrator or management activities of the transmitted nodes (host & router).
Availability	Ensures that the ability to administer or manage the transmitted nodes by authorized entity can not be denied. This includes the protection against the active attacks and passive attacks of the network transmission facilities administrative authentication information.
Non-repudiation	Provides a record identifying the entities or devices performing the administrative or management activity on the network transmitted nodes. This record will be used as proof that the administrative or management activity was performed with an indication of the nodes or network devices that performed it.
Data Confidentiality	Protects all files used in creation and execution of the transmitted nodes from unauthorised access or viewing. This applies to files stored or being transmitted across the network. Protects the nodes' administrative or management information (e.g. user identification and passwords, administrator identification and passwords) from unauthorised access or viewing.
Data Integrity	Ensures that all files used in creation execution of transmitted nodes can not be modified, deleted, created or replicated. This protection applies to the files inhabitant in nodes and network devices, being transmitted across the network or stored as offline.
Privacy	Protects the information that can be used to identify the transmitted nodes from unauthorised entities.

Table 4.5: Applying security requirements to the Routing Layer, Management Plane

Securing the end-user plane of the Routing layer is concerned with securing the user-data of the transmitting nodes. **Table 4.6** shows the objectives of applying the security requirements to the routing layer in the end-user plane.

Proceed 6: Routing Layer & End-User Plane	
Security REQ.	Security Objectives
Authorisation	Ensures that only authorised nodes can gain access to different end-user data of each transmitted node in the MANoN.
Authentication	Identifies the routing request from the end-user nodes that are attempting to communicate or access end-users data in every transmitted node in the MANoN.
Availability	Ensures the availability between transmitted nodes and services provided (e.g. providing credentials) by them. This includes protection against all active attacks and passive attacks.
Non-repudiation	Provides a record identifying the nodes performing activity on the end-user nodes is actually performed. This record can be used as proof of the access to end-user data.
Data Confidentiality	Ensures that data transferred between the end-users cannot be viewed or understood. Protects the end-user information from unauthorized access or viewing.
Data Integrity	Ensures that the data transferred between the end-user nodes are not modified, deleted, created or replicated. This applies to the configuration information resident in nodes and network devices being transmitted across the network or stored offline.
Privacy	Protects the information that can be used to identify end-user nodes and their network devices (transmission facilities), base station location and identity from unauthorised nodes.

Table 4.6: Applying security requirements to the Routing Layer, End-user Plane

Securing the management plane of the application layer is concerned with securing the operations, administration, maintenance, and provisioning (OAM&P) of the nodes application (SSL and SSH). **Table 4.7** shows the objectives of applying the security requirements to the Application layer in the management plane.

Proceed 7: Application Layer & Management Plane	
Security REQ.	Security Objectives
Authorisation	Ensures that only high priority nodes are authorised to perform administrator or management activities of the network-based applications.
Authentication	Ensures that the identities performing administrator or management activities on nodes or network devices are who they claim to be in each MANET.
Availability	Ensures the availability of high priority nodes and applications provided by them. This includes protection against all active attacks and passive attacks of the administrative authentication information.
Non-repudiation	Provides a record identifying the nodes performing administrative or management activity on the nodes or applications and the action that was performed. This record can be used as proof of the originator of the administrative or management activity.
Data Confidentiality	Ensures that data transferred between the administrative entities cannot be viewed or understood. This applies to application files resident in network devices, being transmitted across the network or stored offline.
Data Integrity	Ensures that the data transferred between the administrator nodes are not modified, deleted, created or replicated. This applies to application files resident in network devices, being transmitted across the network or stored offline.
Privacy	Protects the information that can be used to identify high priority nodes and their applications from unauthorised nodes.

Table 4.7: Applying security requirements to the Application Layer, Management Plane

Securing the management plane of the application layer is concerned with securing user-data provided to the node applications. **Table 4.8** shows the objectives of applying the security requirements to the application layer in the end-user plane.

Proceed 8: Application Layer & End-user Plane

Security REQ.	Security Objectives
Authorisation	Ensures that only authorised nodes are able to access and use network-based applications.
Authentication	Verifies the identities of nodes attempting to access or use network-based applications.
Availability	Ensures that the access of network-based application by end nodes cannot be denied. This includes protection against all active attacks and passive attacks of the administrative authentication information.
Non-repudiation	Provides a record identifying the end nodes activity on the network-based applications and the action that was performed. This record will be used as proof of access to and use of the application by the end node.
Data Confidentiality	Ensures that data transferred between the end-user entities cannot be viewed or understood. This applies to application files resident in network devices, being transmitted across the network or stored offline.
Data Integrity	Ensures that the data transferred between the end-user nodes are not modified, deleted, created or replicated. This applies to the application files resident in network devices, being transmitted across the network or stored offline.
Privacy	Protects the information that can be used to identify end user nodes and their applications from unauthorised nodes.

Table 4.8: Applying security requirements to the Application Layer, Management Plane

Attacks on a MANoN attempt to evade security requirements (authorisation, authentication, privacy, data confidentiality, availability, data integrity, and non-repudiation), which are defined in the Security Architecture for MANoN.

In order to satisfy the objectives of the security requirements (section 4.2.1) and protect MANoN from various types of security attacks, there are various technologies that can be used. **Table 4.9** shows examples of some of these technologies.

These technologies could be applied to satisfy the objectives of the security requirements in the eight proceeds explained above. The specification of each technology and the way of applying it varies from proceed to proceed and between security requirements.

The next chapter will introduce a novel ***Access Control Mechanism and Behavioural Detection technique for Managing Digital Certificates in the State-of-the-art MANoN*** fulfilling the objectives of *authentication, authorisation, availability, data confidentiality, data integrity and non-repudiation* at proceeds (1, 2, 7, 8).

Security Requirements	**Technique Used**
Authorisation	Password, Access Control List (ACL), Firewall
Authentication	Shared Secret, Public Key Infrastructure (PKI), Digital signatures, digital certificate
Privacy	(Partially by) Encryption, Mechanisms to hide locations and Routing protocols used
Data confidentiality	Encryption

Availability	Intrusion Detection Systems/ Intrusion Prevention Systems (IDS/ IPS)
Data Integrity	Hash functions, Digital certificate
Non-repudiation	Digital Signatures, System logs

Table 4.9: Technologies for satisfying Security Requirements

4.5 Summary

A security architecture for MANoN is proposed. The security architecture presents a comprehensive, end-to-end high level security solution for MANoN that could be applied to any wireless service provision scenario exploiting MANoN in order to predict, detect and correct security vulnerabilities.

The security architecture is defined upon the ITU-T recommendations, X.800 and X.805. The proposed security architecture identifies seven security requirements that protect the system against all major security threats attempting to attack MANoN. Attacks on MANoN are characterised by accidental or intentional generation, either internally or externally and the use of active or passive behaviour. We have illustrated a methodical approach for securing MANoN by taking each *Proceed* between any layer and plane as a unique perspective, with consideration for the seven requirements that presented eight tables describing the objectives of the security requirements for each Proceed.

Finally, the application of the proposed security for MANoN in order to achieve end-to-end security solutions for MANoN using different technologies is explained.

Chapter 5

Security Management Techniques

Objectives

- Define our security management components upon recommendation ITU M.3400
- Present an introduction to our security mechanisms ACM-MANoN and BD-MANoN
- Present the methodology used to evaluate our security mechanisms
- Propose the parameter values used in the NS-2 simulation environment
- Design our MANoN system model

5.1 Introduction

The previous chapter presented the Security Architecture that provides a comprehensive, end-to-end security solution for MANoN. In order to satisfy the objectives of the security requirements defined in this architecture, we need to propose a set of mechanisms to enforce these security requirements, and forestall any attempts to evade them; but first of all, we need to explain and define our system, to find whether our MANoN is a burden or advantage to the real life situations and how these security mechanisms could be implemented for a MANoN, which will be explained later in this chapter. Moreover, we will highlight the main points for implementing a comprehensive securely managed system.

This chapter presents a novel security-management system based upon Recommendation ITU-T M.3400 [58], which is used to evaluate, report on the behaviour of our MANoN and support the complex services our system might need to accomplish.

In this chapter, novel security mechanisms are used to satisfy the objectives of security requirements such as *authentication, authorisation, availability, data integrity, and non-repudiation* in Proceed (1), Proceed (2), Proceed (7) and Proceed (8) previously defined in Chapter 4.

In the present chapter, we propose novel, efficient *security mechanisms for managing digital certificates in MANoN*. We will assume that MANoNs are operating in heterogeneous wireless environments such as WLANs and cellular systems. We define two different algorithms for two different scenarios.

The first algorithm manages digital certificates when all ad hoc nodes are part of other infrastructure-based wireless networks, meaning that all nodes are defined and known to each other in the MANoN (***Access Control Mechanism for MANoNs (ACM-MANoN)***). This algorithm is based on the hierarchical trust model used with threshold cryptography as our PKI, to provide a high level of secure, available and well managed certification service.

The second algorithm assumes that some of the ad hoc nodes are present in other wireless networks, meaning that only some of the nodes are defined in our MANoN. In this case, the mechanism will be a combination of behaviour detection and threshold cryptography (***Behaviour Detection for MANoN (BD-MANoN)***); in other words the digital certificates will be managed by a behaviour detection algorithm. The following two chapters will prove that the proposed mechanism is still fully distributed and that it provides a high level of secure, available, scalable and efficient management services for MANoN.

The rest of the chapter is organised as follows: Section 5.2 presents a new security mechanism for managing digital certificates in MANoN. It explains how this mechanism implements the security requirements, as well as identifying two algorithms for two different scenarios in the security mechanism. Section 5.3 describes the evaluation methodologies we used to test the performance of the proposed security mechanism. Finally, the outcomes are summarised.

5.2 Securely Managing MANoN

Providing security management is critical for any system, and our MANoN is not exceptional; our security management will be described upon the Recommendation ITU-T M.3400 perspective, showing three essential components:

- *Security Administration*
- *Prevention and Detection*
- *Containment and Recovery*

In any system, providing one of those components is a problem, but if we are dealing with an infrastructure-less MANoN, it will be a dilemma, yet we approached each set group independently, providing unusual solutions for each one of them.

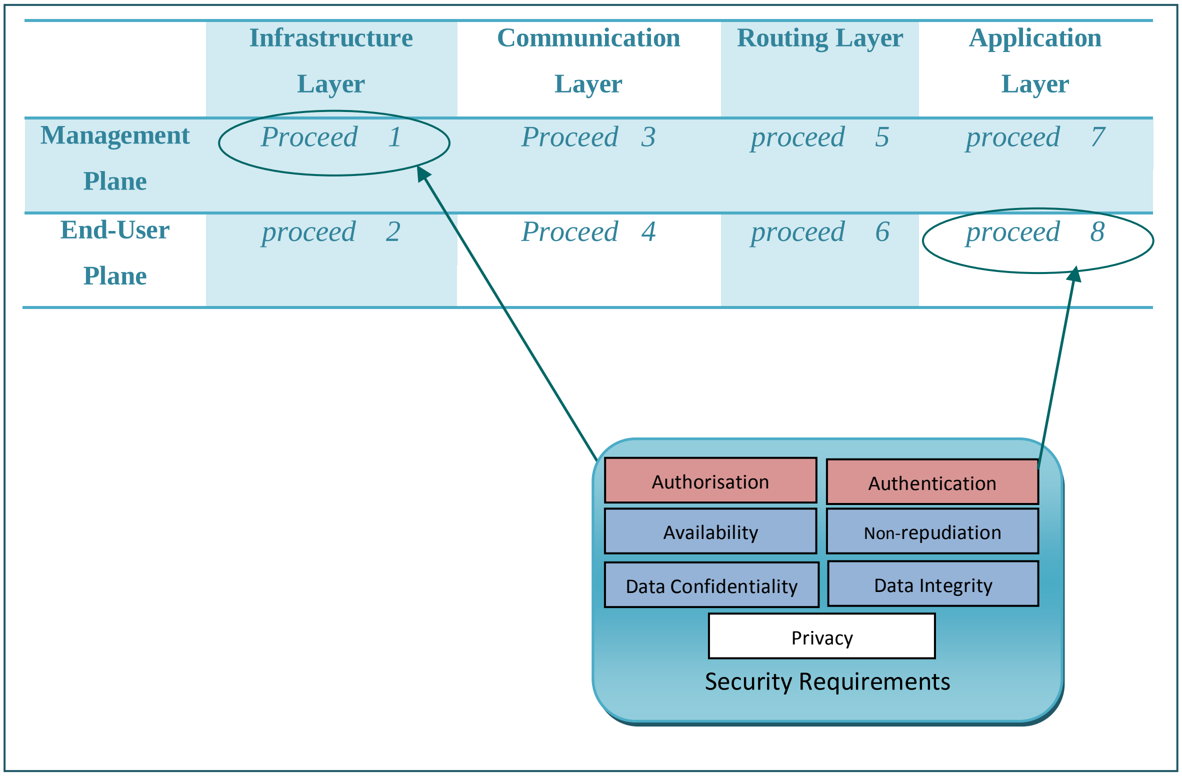
The *Security Administration* function sets are those needed for planning and administrating security policies and managing security related information. Owing to the lack of underlying infrastructure, depending on a central administration is impossible, raising one of the major issues ad hoc networks might face [99]. That is why we employ threshold cryptography as our key management service, and a distributed authority inherits a number of CA nodes (explained in detail in chapter 6 and chapter 7) with higher computational power delegated to carry out the administration duty, which will be known as Back Bone Nodes (BBN).

Prevention and Detection, the prevention function sets, are those needed to prevent intrusion, whereas detection function sets are those needed to detect an intrusion. To prevent or detect illegitimate users, the security requirements must be defined and satisfied; therefore, we designed novel security mechanisms to satisfy these requirements. Chapter 6 explains our prevention mechanism, which is based on *authentication* and *authorisation* digital certificates in a pre-defined MANoN scenario. Meanwhile, chapter 7 illustrates the state-of-the-art behaviour detection algorithm that shows how nodes can act without the need of any strict security mechanisms.

The *Containment and Recovery* function sets are those needed to deny access to an intruder, repair damage done by an intruder, recover losses and to update the system whenever needed. As known, providing an online periodic system to our infrastructure-less MANoN is already complicated enough; in chapter 6, our MANoN scenario shows that some nodes have a high-level transmission facility, enabling them to connect through other heterogeneous networks, such as satellite, unmanned aerial vehicle, or cellular (demonstrated in chapter 6) networks, to obtain an online periodic system.

5.3 Implementing Security Requirements Defined in the Security Architecture

Various technologies can be used to implement the security requirements defined previously in Chapter 4. Modern cryptography – including public key cryptography, digital signatures and digital certificates – are the most powerful tools that can be used to implement most security requirements, including authentication, authorisation, data confidentiality, data integrity and non-repudiation.



	Infrastructure Layer	Communication Layer	Routing Layer	Application Layer
Management Plane	*Proceed 1*	*Proceed 3*	*proceed 5*	*proceed 7*
End-User Plane	*proceed 2*	*Proceed 4*	*proceed 6*	*proceed 8*

Figure 5.1: The implementation of the security requirements using the proposed security mechanisms

The unique characteristics of MANoN make the application of these technologies a real challenge. This issue is tackled in this chapter by proposing new security mechanisms, namely the access control and behaviour detection mechanisms.

The proposed security mechanisms will focus on the proceeds of the trust infrastructure and application layers (proceeds 1, 2, 7, 8) defined in the previous chapter. This is because of the importance of this object in representing the main functionalities of MANoN as wireless access networks. As shown in Figure 5.1, the security mechanisms will satisfy *authentication* and *authorisation*, and help toward forcing other security requirements such as *availability*, *data confidentiality*, *availability*, *data integrity* and *non-repudiation*. Chapter 6 and 7 will highlight these requirements, showing how our security mechanisms are satisfying these requirements.

5.4 MANoN System Model

Our system model involves a number of autonomous nodes interconnecting with each other by wireless communication in a heterogeneous environment. Each node is an ad hoc network, which has the ability to operate separately with its own supervision and management, creating what is known as MANoN. Each network has the ability to disconnect and join on different bases without affecting the main system. We have defined two scenarios for our MANoN:

First, all the MANETs are pre-connected by wireless connection to exchange data, and to update information on each other (e.g. private and public keys).

In the second place, not all MANETs are predefined in the MANoN community. Figure 5.2 shows the two types of MANoN scenario.

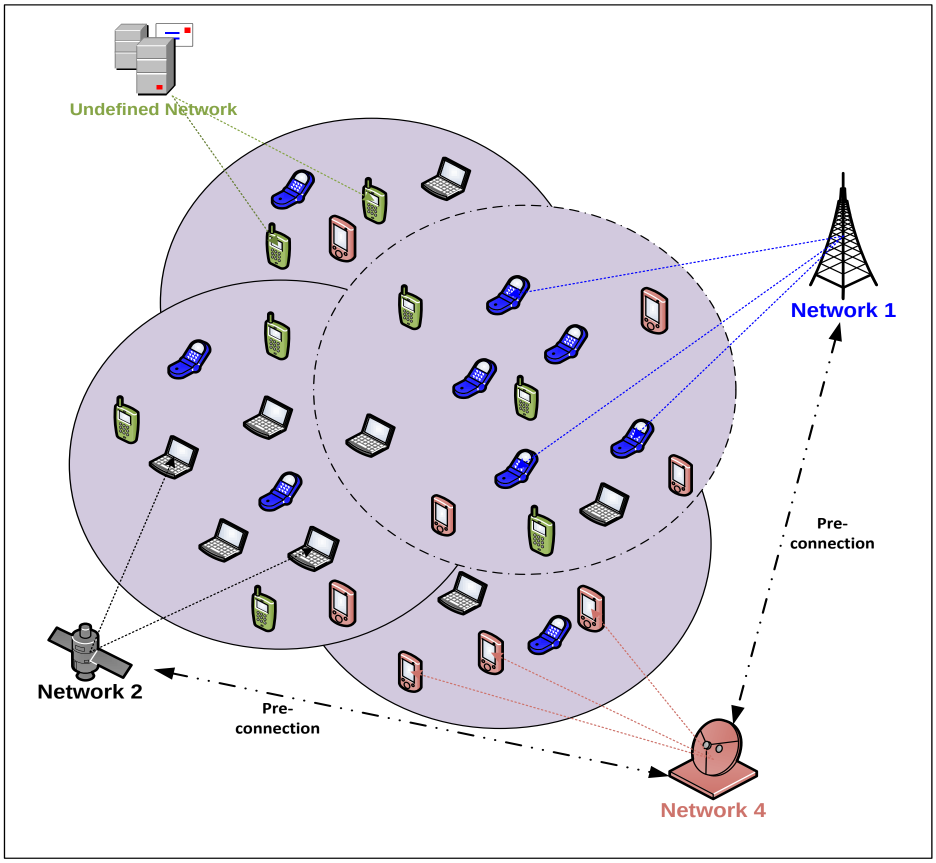


Figure 5.2: MANoN two scenarios

5.5 Security Mechanisms Evaluation

This section discusses the methodology used to evaluate the performance of the proposed security mechanism ***ACM-MANoN***. It shows what the evaluation metrics are and which simulation environments are used to test them, as shown in Figure 5.3.

5.5.1 NS-2 Based Evaluation

The behaviour of the ***ACM-MANoN*** in real network environments needs to be tested, the overhead caused by this security protocol measured and the time needed to perform successful certificate authentication services calculated. Therefore, a suitable network simulator must be chosen to provide the communication performance of the proposed security mechanism. This section will justify the application of the NS-2 simulator to simulate the security mechanism, as well as showing how the simulation environment is set, what the simulation metrics are and what parameter values have been used.

5.5.2 Network Simulator: NS-2

In order to evaluate the performance of the security mechanism ***ACM-MANoN***, in terms of communication cost, they must be implemented using one of the available network simulators suitable for simulating such types of wireless network.

Many researchers in MANET have evaluated and simulated their work using various approaches and simulation tools. The most popular network simulators are Network Simulator-2 (NS-2) [112, 29, 5], Global Mobile Information System Simulation Library (GloMoSim) [37] and OPNET Modeler [84]. Some work has been simulated using self-developed code.

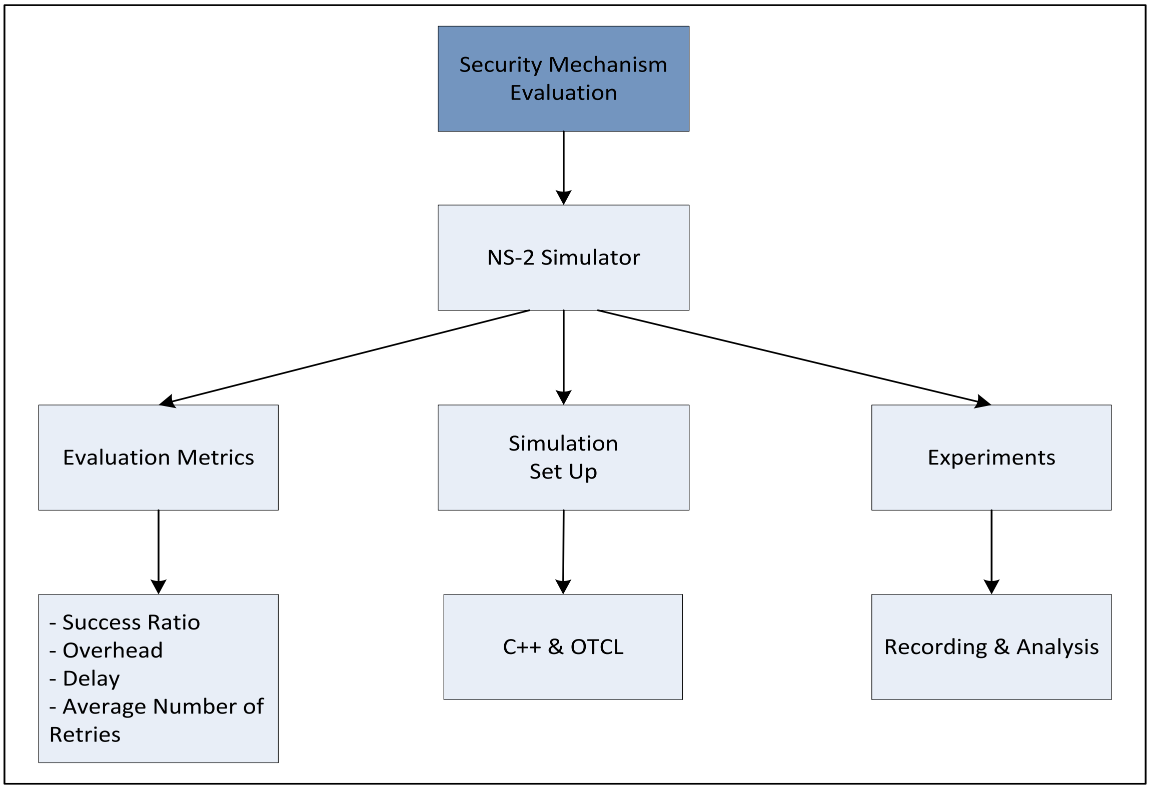


Figure 5.3: Security mechanism evaluation

The authors in [62] surveyed the 2000-2005 proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc). They found that NS-2 is the most frequently used of all simulators in MANET research: “35 of the 80 simulation papers that state the simulator used in the simulation study used NS-2 (43.8%)”, as shown in Figure 5.4.

NS-2 has been chosen to simulate the ***ACM-MANoN*** in the present research. What distinguishes NS-2 from other simulators is the range of features it provides and its open source code that can be modified and extended. It provides substantial support for the simulation of TCP, routing and multicast protocols over wired and wireless (local and satellite) networks.

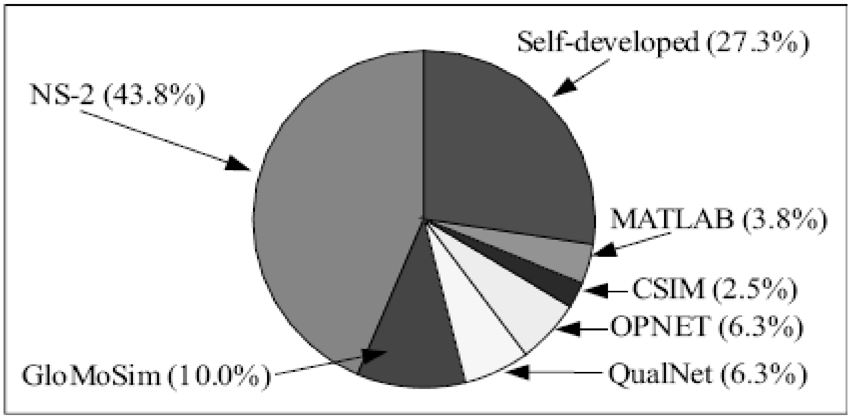


Figure 5.4: Simulator usage from MobiHoc survey [62]

NS-2 is a discrete event and an object-oriented simulator targeted at networking research; it was developed by the University of California at Berkeley and the VINT project [112]. There are several versions of NS-2. We have used version NS-2.31 in our simulation. The simulator is installed on the Linux-based operating system **Ubuntu 7.10**.

The NS-2 simulator is based on two languages: an object oriented simulator, written in C++, and an OTcl (an object oriented extension of Tcl) interpreter, used to execute the user's command scripts. It has a rich library of network and protocol objects. There are two-class hierarchies: the compiled C++ hierarchy and the interpreted OTcl, with one-to-one correspondence between them. The compiled C++ hierarchy allows us to achieve efficient simulation and faster execution times. This is particularly useful for the detailed definition and operation of protocols, allowing the reduction of packet and event processing time.

In the OTcl script provided by the user, we can define a particular network topology, the specific protocols and applications we wish to simulate (and whose behaviour has already been defined in the compiled hierarchy) and the form of the output that we wish to obtain from the simulator. The OTcl can make use of the objects compiled in C++

through an OTcl linkage (done using tclCL: a Tcl/C++ interface [111]) that creates a matching of OTcl object for each of the C++. Therefore, from the user's perspective, NS-2 is an OTcl interpreter that takes an OTcl script as input, and produces a trace file as output (Figure 5.5).

One of the compensations of this split-language programming is that it allows for the fast generation of large scenarios. This is because NS-2 can efficiently manipulate bytes and packet headers, and implement algorithms that run over large data sets. For these tasks, run-time speed is important. C++ is slow to modify, but its speed makes it appropriate for protocol implementation. On the other hand, a large element of network research involves slightly changing parameters and configurations, or exploring a number of scenarios. In these cases, iteration time (change the model and re-run) is more significant. Since configuration runs once (at the beginning of the simulations), run-time of this part is less important. OTcl runs slower but can be altered very quickly making it ideal for simulation configuration.

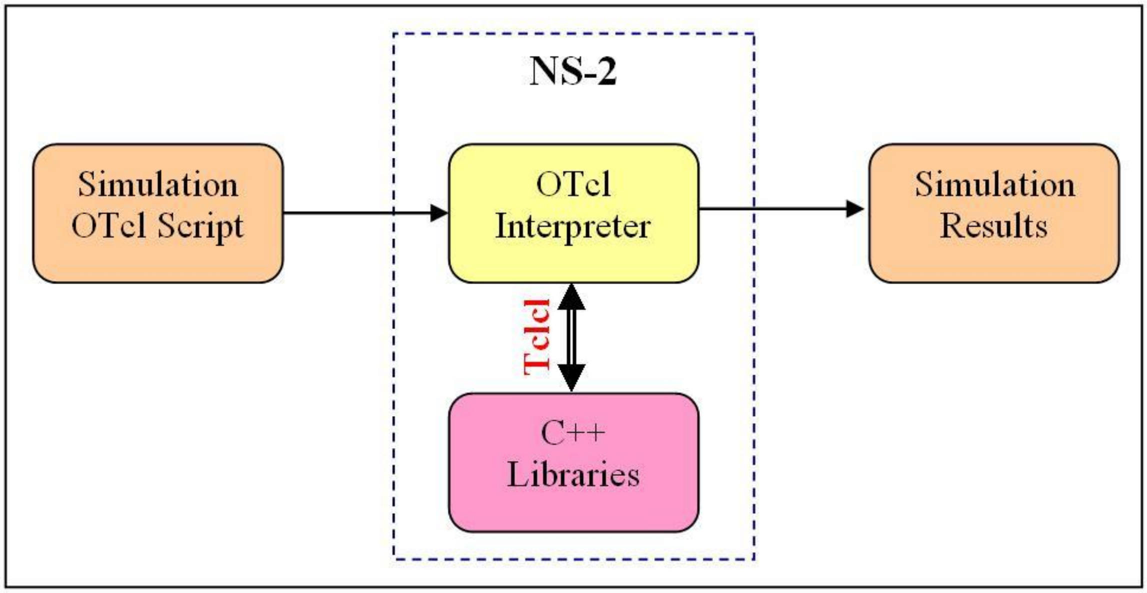


Figure 5.5: Schematic structure for NS-2

5.5.3 Simulation Environment of the Security Mechanism

A TCL script file for mobile ad hoc wireless simulations provided by the NS-2 distribution was modified to fit the simulation environment of the security mechanism. In this file, it was necessary to define the type of each of the network components that nodes compromise. A mobile node consists of network components such as Link Layer (LL), Interface Queue (IfQ), MAC layer and the wireless channel from which nodes transmit and receive signals. In addition, in the TCL script file, it is necessary to define other parameters such as type of antenna, radio-propagation model and type of ad-hoc routing protocol used by mobile nodes.

The size of trace files generated by running the TCL script file is huge – of the order of tens of megabytes. The total size of all trace files generated in all experiments of the ACM-MANoNs algorithm is around ***31 GB***. These files were analysed to obtain the performance metrics. In order to extract certain lines and discard the rest from the generated trace file for analysis, the "**grep"** UNIX command was used. Grep [84] is the most useful command provided by the UNIX operating system, and allows file filtering.

A new file consisting only of those lines from the original file that contain a given character sequence can be created. For example, the output traces in NS-2 might contain all the types of packet that are part of protocols such as the routing and MAC protocols, while the present work concerns itself only with the packets generated by the security protocols that implement the two algorithms. In this case, only the required information need to be filtered from these trace files. Subsequently, a visual basic tool has been developed to take those filtered files as an input, and then calculates the evaluation metrics of the two algorithms. An example of using this tool will be discussed in the next two chapters.

5.5.3.1 Simulation Environment of the Security Mechanism

The following metrics are used to evaluate the proposed security mechanism in terms of communication cost. **Success Ratio** measures the ratio of the number of successful certificate authentication requests over the total number of certificate authentication requests that should take place during the simulation time. **Average Delay** measures the average latency to authenticate a certificate successfully. **Overhead** measures the total number of packets transmitted as part of the security protocol (ACM-MANoNs) that provides certificate authentication for MANoN nodes. Finally, **Average Number of Retries** measures the average number of retries before a node successfully authenticates a certificate.

Each metric mentioned above has been simulated in three different scenarios: the **mobility scenarios** with different pause time values (0, 10, 40, 60, 100), the **speed scenarios** with different node speeds (1, 10, 15, 20, 25, 30), and the **network size scenarios** with different numbers of nodes (10, 20, 40, 60).

The other factors affecting the performance of the security algorithms ACM-MANoN need to be justified before using them in the simulation, the details of which will be shown in the next two chapters.

5.5.3.2 Parameters Values

Currently, there is no single benchmark of MANoN scenarios to test a protocol [62]. The MANoNs community needs a way to characterise simulation scenarios in order to evaluate and compare protocols and performance, and to ensure that protocols are rigorously tested.

In an attempt to generate results that would be representative to some potential real world scenarios (which might be encountered by the algorithm), simulations were run with parameter values close to the available real ones. Without loss of generality, the security protocol evaluations are based on the simulation of 50 wireless nodes for some scenarios, and different numbers of nodes varying from 10 to 60 for other scenarios. These nodes form the MANoNs, moving about over an area of 1000m x1000m for 500 seconds of simulated time. The square site models situations in which nodes can move freely around each other, and where there is a small amount of path and spatial diversity available for the routing protocol to discover and use. A 1000m^2 space was chosen because it is four times the transmission range of 250 metres, which allows the possibility of a reasonable number of nodes between the source and destination nodes. This is because a higher number of intermediate nodes results in quicker route breaks. On the other hand, a smaller number of intermediate nodes does not give an indication of the realistic security protocol.

In the simulation model, the mobile nodes are placed randomly within the simulation area. In terms of a mobility model, a Random WayPoint Model (RWP) [111] is used for different values of pause time, maximum node speed, and network size. The random waypoint model is one of the most widely used mobility models in the performance analysis of mobile wireless networks [50]. In the Random WayPoint Model, nodes are initially placed randomly within the simulation field. Each node selects a destination randomly and independently from other nodes, and it moves towards this destination with a constant speed. When a node reaches its destination, it stays there for a given pause time before it starts to move to another random destination. In this manner the pause time value reflects how often nodes move during the scenario, which in turn reflects the amount of topology change.

In order to generate the movement of the mobile nodes, the CMU's scenario- generating scripts have been studied to create these files and make use of the scenario-generation utility “setdest”. The node-movement generator is available under the ~ns/indep-utils/cmu-scen-gen/setdest directory created when NS-2 is installed. The IEEE 802.11 Medium Access Control (MAC) Distributed Coordination Function (DCF) [60] protocol is used in the simulation to get the link breakage feedback signal. The physical radio characteristics of each mobile node's network interface, such as the antenna type, transmit power, and receiver sensitivity, were chosen to approximate the most common commercially available wireless LAN radio, such as the Lucent WaveLAN [106] radio.

The radio propagation range for each node was 250 metres and the channel capacity was 2 Mbps. The propagation model used in the simulation was the two-ray ground reflection model. **Table 5.1** provides a summary of the other simulation parameters.

Scenario Name	***Mobility (Pause Time) Scenario***	***Max Node Speed Scenario***	***Network Size Scenario***
Pause Time (s)	0, 10, 40, 60, 100	10	10
Max Node Speed (M/s)	20	1, 10, 15, 20, 25, 30	20
Number of Mobile Nodes	50	50	10, 20, 40, 60
Simulation Time (s)	500	500	500
Network Space (m)	1000 x 1000	1000 x 1000	1000 x 1000
Radio Range	250m	250m	250m
MAC Protocol	IEEE 802.11	IEEE802.11	IEEE802.11
Radio Propagation Model	two-ray	two-ray	two-ray
Antenna Model	Omni Antenna	Omni Antenna	Omni Antenna

Table 5.1: The parameter values used in NS-2 based simulation

5.6 Summary

This chapter presented an overview of new security mechanisms for securely managing MANoN. These security mechanisms implement the objectives of *authentication, authorisation, availability, data confidentiality, data integrity and non-repudiation* of proceeds (1), proceeds (2), proceeds (7), and proceeds (8), as defined in Chapter 4.

The security mechanisms assume a heterogonous wireless environment in which MANoNs are operating in an area covered by other infrastructure-based wireless networks, such as WLANs and cellular systems. Those security mechanisms propose two algorithms for two different scenarios.

The first algorithm, called ***ACM-MANoN***, tackles the issue of managing digital certificates where all MANET nodes are participating at the same time in other infrastructure-based wireless networks. The key management system in this case will use the threshold cryptography PKI. This algorithm, as will be shown in the next chapter, will provide a high security, efficient, distributed and scalable key management service with high availability.

The second algorithm, ***BD-MANoN***, assumes as a part of its network model that some MANET nodes belong to other existing and defined wireless networks. This security mechanism depends basically on nodes behaviour to decide whether the nature of each node is malicious or normal. This combination will be shown in Chapter 7.

Chapter 6

Algorithm1: Access Control Mechanism for MANoN (ACM-MANoN)

Objectives

- Define the prevention component for our MANoN
- Describing our ACM-MANoN in a heterogeneous environment using threshold cryptography as key management service
- Implementing our ACM-MANoN
- Describing our ACM-MANoN in a formal description method
- Evaluating our ACM-MANoN using NS-2 base simulation

6.1 Introduction

The integration of heterogeneous wireless technologies can improve network performance, thereby meeting different security requirements as will be shown in this chapter. The research into integrating ad hoc networks with other wireless networks such as cellular networks can be found in [71,47]. These focus on how MANoN can enhance cellular services.

This chapter will examine the integration of heterogeneous wireless networks to enhance the performance of MANoN from a security perspective. It proposes a novel integrated access control mechanism system to improve the security level in the new type MANoN. The access control mechanism is based on threshold cryptography to achieve prevention techniques providing a high level of security management, availability and a management certification service for pre-defined nodes of the MANoN.

The following sections present the network and system model constituting the basis of ACM-MANoN. The ACM-MANoN certificates management framework is defined and the means of coping with misbehaving nodes in this algorithm is explained. Finally, ACM-MANoN will be evaluated and the obtained results are discussed and analysed.

6.2 Network and System Model

In this algorithm all the nodes comprising the ad hoc networks are involved in other infrastructure-based wireless networks such as WLAN and cellular systems. Therefore, each of the ad hoc nodes will belong to a PKI (MANET) creating the MANoN system, as shown in Figure 6.1.

Our MANoN involves a number of MANET interconnecting with each other; in addition all PKI are pre-connected by wireless connection to exchange data, and to update information. Each PKI has a set of *(t+1)* CAs (Servers CA_{Se} and Combiners CA_c) acting as administrators known as Back Bone Nodes (BBN). Those CAs are fully trusted by all nodes that belong to this PKI. It is relatively uncommon to have one node that belongs originally to more than one PKI, because this protocol is used either in civilian or military environments where the number of PKI within a given area is limited.

This will include the PKI of the known mobile operators and wireless LANs in that area. For example, there is no common node that belongs to both the mobile operator Orange and O_2, or two nodes belong to the both UK and US army.

6.3 ACM- MANoN Certificate Management Framework

This section describes the certificate management system of ACM-MANoN. It shows how public/private keys and digital certificates are created, presents the formalisation code of the ACM-MANoN algorithm. It also illustrates the process of certificate revocation.

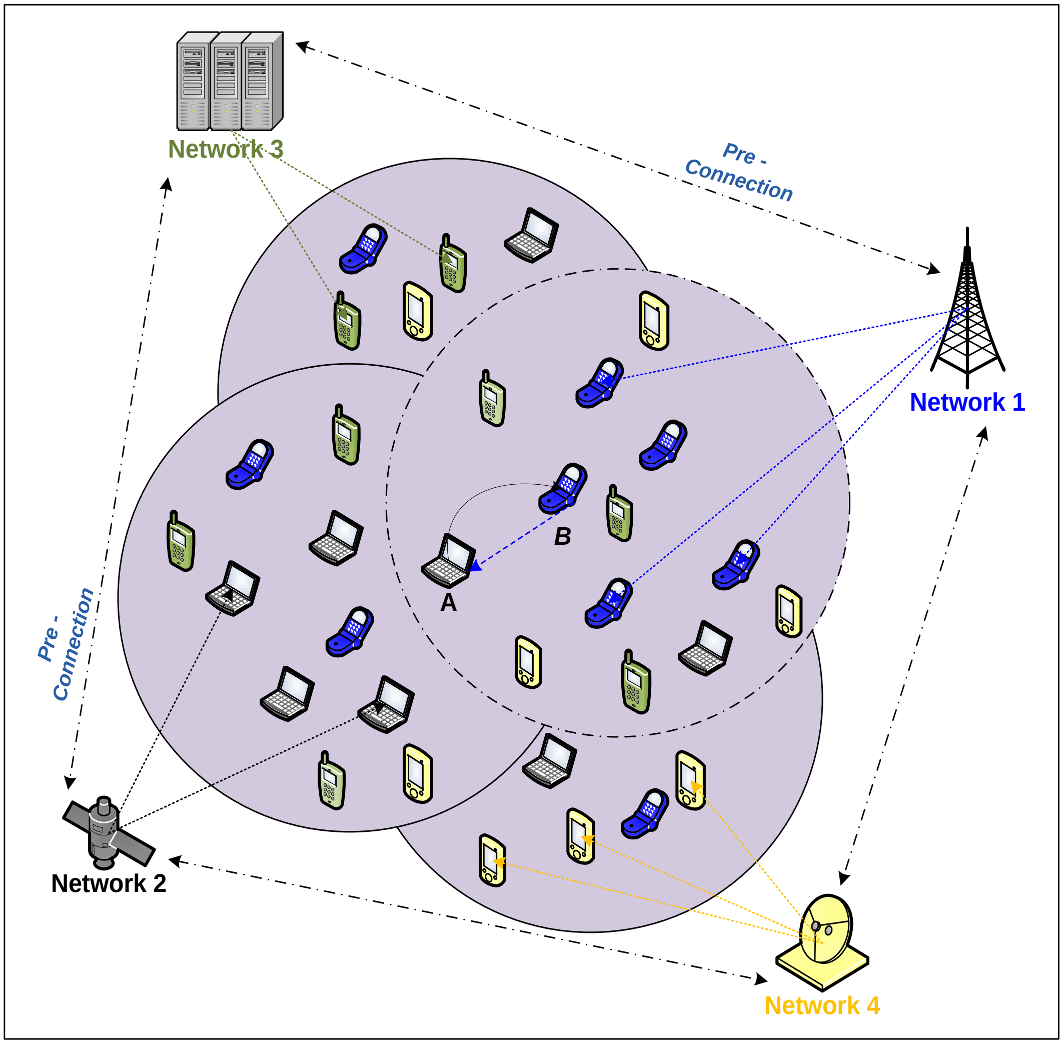


Figure 6.1: Network Model of ACM-MANoN

6.3.1 Creation of Public/ Private Keys and Digital Certificates

The use of our ACM-MANoN requires a key management service. We adopt PKI because of its superiority in distributing keys, and achieving integrity and non-repudiation. In PKI, each node has its own Public/ Private key pair. Public keys can be distributed to other node, while private keys should be kept confidential to individual nodes.

As mentioned each node has its own Public/ Private keys, each node will receive its own Authentication and Authorisation certificates from its own PKI (MANET). The Authentication certificate will be used as an Identity (Passport), whereas Authorisation certificate will be used as a security clearance. Each MANoN's node will hold its certificate in a Local Data Base (LDB). The main structure of ACM-MANoN digital certificates is shown in Figure 6.2.

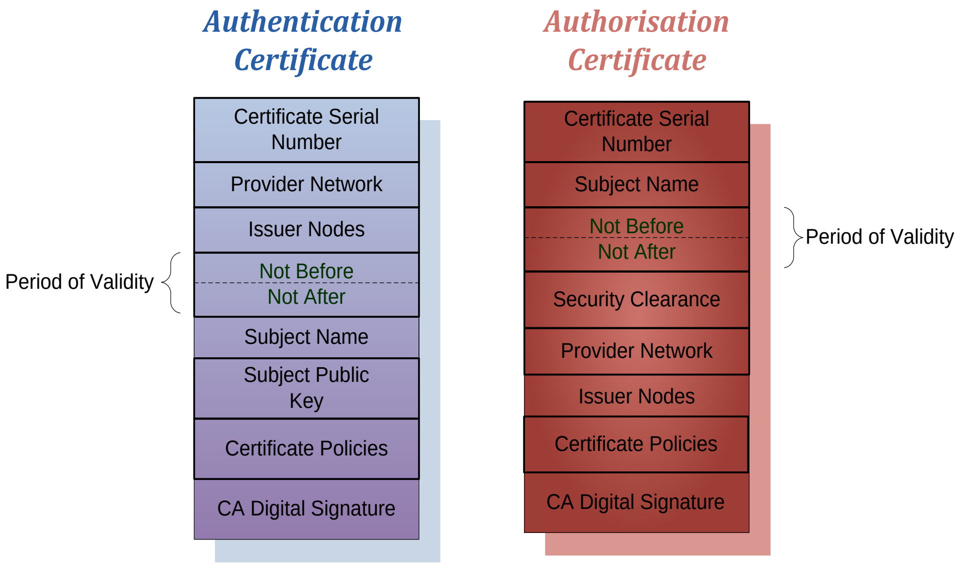


Figure 6.2: The Structure of ACM-MANoN Digital Certificates

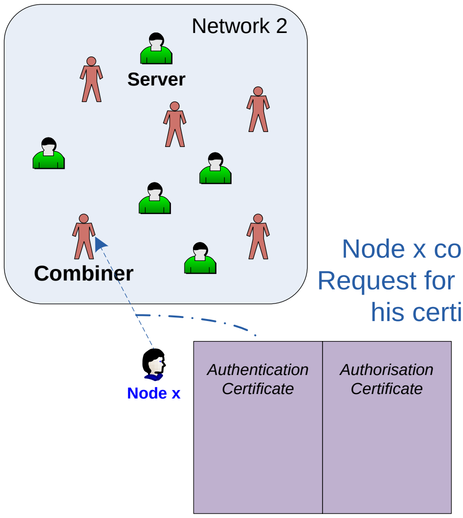
The certificates contain:

- ***Serial number:*** A unique integer value within the issuing PKI or CA (servers and combiners), that is unambiguously associated with the certificate.
- ***Provider Network:*** Name of the network that issued the certificate.
- ***Issuer Nodes:*** PKI or CA names that created and signed the certificate.
- ***Period of Validity:*** Consist of two dates: the first and last on which the certificate is valid.
- ***Subject Name:*** Holder of the certificates.
- ***Subject's Public-key:*** The public key of the user.
- ***Security Clearance:*** Level of the authorisation certificate which allow the subject to perform in any network with the same priority level (i.e. nodes in a specific network).
- ***Certificate Policies:*** Certificates may be used in environments where multiple policies apply. So, this section will carry list of policies that the certificate recognised as supporting, together with optional qualifier information.
- ***CA Digital Signature:*** Digital signature being signed either by the PKI or the CAs.

6.3.2 ACM-MANoN Implementation

As mentioned all nodes receive their keys and certificates (*Authentication*, *Authorisation*) from their PKI, moreover, MANoN service has its own Public/ Private keys, all CAs (*Servers CA_{Se}* , *Combiners CA_{C}*) will receive a share of the private key (to sign certificates and perform threshold cryptography) and the public key in order for the CA_S to be able validate other MANoN certificates.

In this scenario network (1) and network (2) are defined in our MANoN system (public keys are exchanged between the CAs), so when node x from network (1) is trying to engage and communicate with node y from network (2), node x will broadcast his request for an authorisation certificate (to perform in network (2)) attached with his own authorisation and authentication certificates that he had received from his original network, as shown below in Figure 6.3.

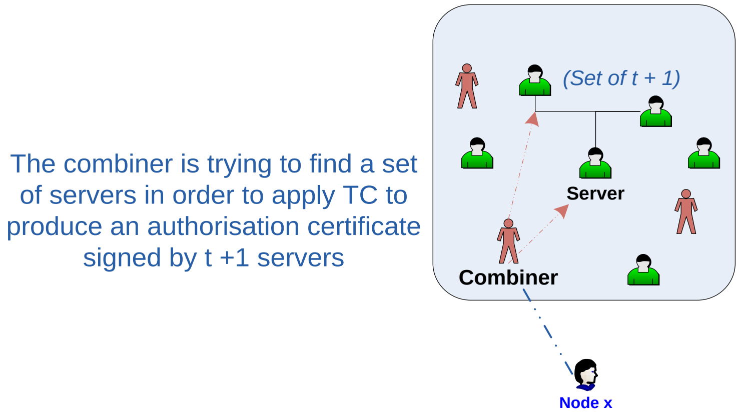


The combiner is trying to validate node's x certificates with the service Public Key of node x

Node x combine his Request for access with his certificates.

Figure 6.3: Request & Validation of the certificates

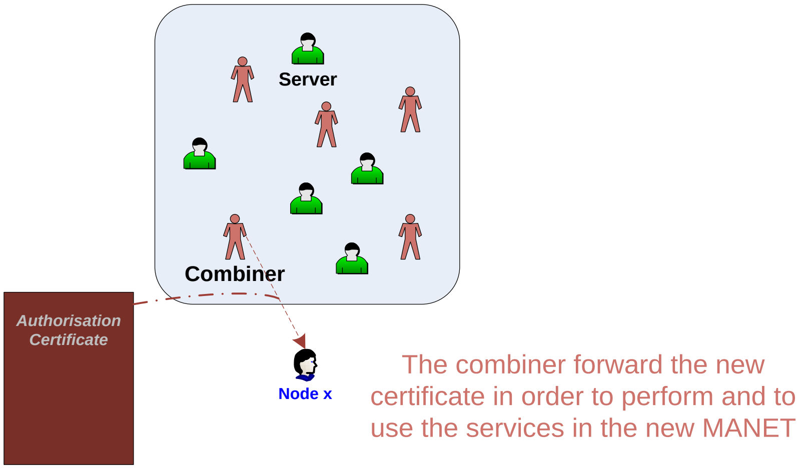
After receiving the request from node x, the CA_C in the correspondent network (Network 2) will validate the certificates by using the service public-key P_{PKI1} that node x belongs to, as shown in Figure 6.3. If the certificates are valid the CA_C tries to find a set of $(t + 1)$ correct partial signatures to generate a digital signature by the CA_S (performing threshold cryptography) in order to create an authorisation certificate with a specific degree of security clearance depending on the security clearance (Certificate Policies) node x certificate carries, as shown in Figure 6.4.



The combiner is trying to find a set of servers in order to apply TC to produce an authorisation certificate signed by t +1 servers

Figure 6.4: Finding a set of legitimate users in order to perform TC

After creating the authorisation certificate the combiner will forward the certificate to node x in order to use it in the network (2). As shown in Figure 6.5. This algorithm is shown in our publication [4].



The combiner forward the new certificate in order to perform and to use the services in the new MANET

Figure 6.5: Forwarding the Authorisation certificate to the requesting node

It is important to check the validity of a certificate, to ensure it is not expired. Therefore, a request for a certificate could be made when it is expired and needs to be renewed, therefore if the confirmation of certificates is invalid either for lack of information (non-predefined network) or expiration, then the request will be rejected and the new authorisation certificate will not be produced. Moreover, the security clearance of any authorisation certificate must be clarified depending on the network it belongs to and the network it is performing in.

Let us suppose that node x from US network is carrying an authorisation certificate of rank D (A is highest Z is lowest) if node x is trying to perform in France network the new authorisation certificate, which will be issued by France will carry Class C (depending on the policy defined & priority difference) giving node x a higher priority to perform in France (as France is defined as less priority then US).

In the implementation of the ACM-MANoN, MANoN nodes try three times to authenticate a key. The reason of choosing three retries will be justified in the evaluation section. The time between each retry and the next one is called the Authentication Time Interval (ATI). After the three retries, if the authentication still can not be validated, authentication of this node has failed. The ACM-MANoN formal description is shown below.

The following variables represent the parameters of the ACM-MANoN:

- n: number of networks in the MANoN; Networks are numbered from 1 to n;
- n_i: number of nodes, including certificate authorities, in the network i, $1 \leq i \leq n$; Nodes in a network i are numbered from 1 to n_i;
- t_i: number of certificate authority servers in the network i, $1 \leq i \leq n$;
- CAS_{ij}: certificate authority server j of the network i, for $1 \leq j \leq t_i$ and $1 \leq i \leq n$;
- CAC_i: certificate authority combiner of the network i, for $1 \leq i \leq n$;
- DC_{xij}: authentication digital certificate of the node j in the network i, for $1 \leq j \leq n_i$ and $1 \leq i \leq n$;
- DC_{yij}: authorisation digital certificate of the node j in the network i, for $1 \leq j \leq n_i$ and $1 \leq i \leq n$;

- Pb_{ij} : public key of the node j in the network i, for $1 \leq j \leq n_i$ and $1 \leq i \leq n$;
- Pr_{ij} : private key of the node j in the network i, for $1 \leq j \leq n_i$ and $1 \leq i \leq n$;
- Pk_i: public key of network i, $1 \leq i \leq n$;
- S_{ij} : share for the certificate authority j of the private key of network i, for $1 \leq j \leq t_i$ and $1 \leq i \leq n$;

Before defining our access control mechanism, healthiness conditions for the variable above must be defined.

- $Pb_{ij} \neq Pb_{uv}$ for $i \neq u$ or $j \neq v$
- $Pr_i \neq Pr_j$ for $i \neq j$
- $Pk_i \neq Pk_j$ for $i \neq j$

After showing the healthiness of our variables, our access control mechanism can be described by the following steps, where T^i denoted the ith component of a tuple T:

1. Granting certificate authority duties to nodes:

$$\forall i, j. (1 \leq j \leq n_i) \wedge (1 \leq i \leq n) \wedge \left(CAS_{ij} = t_i\right) \wedge (CAC_i = t_i + 1). \quad (1)$$

   Here we choose the high ranked t_i nodes of each network i to play each the role of *Certificate Authority Server* and the node $t_i + 1$ to be the *Certificate Authority Combiner*, for the network *i*.

2. Issuing digital certificates to local nodes of each network:

$$\forall i, j. \Big((1 \leq j \leq n_i) \wedge (1 \leq i \leq n) \wedge \left(DC_{xij} =< j, i, sdx_{ij}, edx_{ij}, CAC_i, Pb_{ij}, \ldots, Sigx_{ij} >\right) \wedge \left(DC_{yij} =< j, i, sdy_{ij}, edy_{ij}, CAC_i, Pb_{ij}, c_{ij}, \ldots, Sigy_{ij} >\right).\Big) \quad (2)$$

where c_{ij} is the security clearance of the node j in the network i; sdx_{ij} and edx_{ij} are the start and end date of the authentication digital certificate; sdy_{ij} and edy_{ij} are the start and end date of the authorisation digital certificate; and the digital signature of the certificates $Sigx_{ij}$ and $Sigy_{ij}$ are calculated by the certificate authority combiner CAC_i of the network i by performing a threshold cryptography involving the certificate authority servers CAS_{iv} and their shares S_{iv} of the private key of the network i, for $1 \leq v \leq t_i$.

Each node uses its digital certificates (authentication and authorisation) to request services within the network it belongs to. However, in order to access services in an external network, a node needs to request from that network a new authorisation certificate in order to perform in it.

3. A request for digital certificates from a node j of the network i to an external network can be modeled by a message of the form:

$$\langle\, j, i, X, Y\,\rangle \quad (3)$$

For some authentication digital certificate X and some authorisation certificate Y.

4. Such a request $\langle\, j, i, X, Y\,\rangle$ is checked by the external network's CA combiner as follows:
   a) The requester is the owner of the authentication and authorisation certificates, i.e.

   $$(X^1 = j) \wedge (Y^1 = j);$$

   b) The network of the requester is the network where the digital certificates X and Ywere issued, i.e.

   $$(X^2 = i) \wedge (Y^2 = i);$$

   c) The digital certificates are not expired, i.e.

   $$(X^3 \leq today \ \leq X^4) \wedge (Y^3 \leq today \ \leq Y^4);$$

Were today denotes the current date;

d) The digital certificates X and Y are authentic using the public key Pk_i of the network i and a signature verification algorithm for threshold cryptography.

5. Issuing digital certificates to an external node j of the network i for it to access services in the network k, $k \neq i$. Here, we suppose that the corresponding request has been successfully authenticated and verified as per step 4 above. The node j of the network i will be issued a new authentication $exDC_{xkj}$ and authorisation $exDC_{ykj}$ digital certificates as follows:

$$exDC_{xkj} =< j, i, sdx_{ij}, edx_{ij}, CAC_k, k, \dots, exSig_{xkj} >$$
$$exDC_{ykj} =< j, i, sdy_{ij}, edy_{ij}, CAC_k, c_{kij}, k, \dots, exSig_{ykj} >$$

Where c_{kij} is the security clearance of the node j of the network i in the external network k; and digital certificate of the certificates $exSigx_{kj}$ and $exSigy_{kj}$ are calculated by the certificate authority combiner CAC_k of the network k by performing a threshold cryptography involving the certificate authority servers CAS_{kv} and their shares S_{kv} of the private key of network k, for $1 \leq v \leq t_k$.

6.3.3 Digital Certificates Revocation

Certificate Revocation is one of the basic services that should be provided by any digital certificate management system. In this algorithm there are two types of certificate revocation:

- ***Explicit revocation***: When the CA belonging to PKI revokes a certificate that it has issued for one of its nodes, and sends the corresponding revocation to other nodes belonging to the same network. If this is not possible for any reason such as the nature of the wireless network of this PKI the renewal of this certificate could be ended, resulting in an implicit revocation.

- ***Implicit revocation***: Each certificate is revoked after its expiration time. In general each certificate contains its issuing and validity times as determined by the issuer. Each CA should therefore update the certificates of its nodes before the expiration time.

In both types of revocation, any information provided by the CA to its nodes about any certificate should be distributed through the exchange process. In this way the nodes belonging to other CAs will be provided with this new information.
Consequently, all of a PKI's nodes are informed when any of them carries out an explicit revocation, and their LDBs are subsequently modified. This revocation will be transferred to other PKIs' nodes by certificate exchange.

The CAs of the PKIs are responsible for updating those certificates that have been implicitly revoked. Once the node has got its new certificate it will update its LDB and then communicate the new certificate to its neighbours through the certificate exchange process. If one of the nodes does not receive the new certificate through the exchange and needs to validate the key, the new certificate will be requested from the CAs it self.

6.3.4 Coping with Misbehaving Users

In the ACM-MANoN algorithm, it is a more difficult task for malicious nodes to make other nodes accept false certificates. This is because all the certificates in this algorithm are issued by a professional CAs and PKIs. Nevertheless, dishonest nodes can try to do the following:

1. Issue certificates for itself. Its then signs the certificates with its private key, claims that these certificates are signed by a professional CA or PKI and uses its public key as the CA public key (this is because ACM-MANoN requests that each node must hold the digital certificates and the corresponding public key of the CA).

2. Try to compromise set of CA_S (as our key management service employs *share refreshing*) over long period of time to gain the private key of the service PKI in order to generate certificates signed by the service public key for itself or different users.

All these types of malicious behaviours can be detected and prevented by the ACM-MANoN algorithm. Referring to ACM-MANoN code, which is defined in section 6.3.2, the authentication within different CA of the key of a node, should pass two conditions:

- The signature should be validated with the public key of the service PKI.
- The public key of the CA or PKI should be compared with other public key certificates attached to the certificates issued by the same CA or PKI.

In the *first case,* when any CA attempts to validate this certificate, the validation process will end successfully because the certificate is signed by the private key, which corresponds to the public key attached to the certificate. But there is another condition.

The CA will compare this attached public key with other public keys attached to certificates issued by the same PKI. In this case, there will be a mismatch with the origin. This node will then develop a bad reputation.

In the *second case*, servers compute new shares from old ones in collaboration without disclosing the service private key to any server. The new share constitute a new *(n, t* + 1) sharing of the service private key. After refreshing, servers remove the old shares and use the new ones to generate partial signatures. Because the new shares are independent of the old ones, the adversary cannot combine old shares with new ones to obtain the private key of the service. Thus, the adversary is challenged to compromise set of t+1 servers between the periodic refreshing. This has been explained in chapter 2.

The area that could be covered by the MANoN is limited and consequently, so is the number of PKIs. This includes the number of known mobile operators in this area (cellular systems), as well as the available WLANs that belong to some governmental or commercial places.

Therefore, these CAs should be familiar and pre-determined; consequently, any forged CA should be easily detected, especially if there is cooperation between these networks. This cooperation could benefit not only MANoN but also these infrastructure-based wireless networks.

6.4 ACM-MANoN Evaluation

Chapter 5 described the evaluation of the proposed ACM-MANoN mechanism, using the NS-2 simulator. This section explains the NS-2-based study of the ACM-MANoN algorithm. It shows what evaluation metrics and parameters values are used. The experimental results of the study will also be analysed. Finally, server issues regarding ACM-MANoN are discussed and the outcomes summarised.

6.4.1 NS-2 Based Evaluation

This section tests the performance of ACM-MANoN in real network environments using the NS-2 simulator. The simulation environments, parameter values and evaluation metrics used in the experiments are presented. The results of these experiments will be shown and analysed.

6.4.1.1 Simulation Environment

The version 2.31of NS-2, was used to simulate the ACM-MANoN algorithm. NS-2 simulator is installed in the Linux-based operating system **Ubuntu 7.10.**

In order to reduce the effect of randomisation used in the simulation, each experiment was executed 30 times and the average calculated. Therefore, the size of the trace files containing the experiment results was huge. These trace files were filtered and sent to a Visual Basic tool in order to measure the evaluation metrics.

In order to ensure repeatability, the ACM-MANoN implementation code, the mobility models generated and used in the experiments, tcl scripts and trace files were saved and will be provided for use by the MANoN and MANET community.

6.4.1.2 Evaluation Metrics

In the NS-2 based study, the performance of ACM-MANoN was evaluated using the following metrics:

- **Success Ratio** measures the ratio of the number of successful certificate authentication requests to the total number of certificate authentication requests that took place during the simulation time in addition to the authorisation certificate

- **Average Delay** measures the average latency to successfully authenticate a certificate

- **Overhead** measures the total number of packets transmitted as part of the ACM-MANoN communication protocol to provide certificate authentication and authorisation services

- **Average Number of Retries** measures the average number of attempts made before a node successfully authenticates a certificate

Each metric mentioned above has been simulated in ***three different scenarios*****:**

- **Mobility Scenario** with different pause time values (0, 10, 40, 60, 100)
- **Speed Scenario** with different node speeds (1, 10, 15, 20, 25, 30)
- **Network Sizes Scenario** with different number of nodes (10, 20, 40, 60)

The other factors affecting the performance of the ACM-MANoN algorithm, which need to be justified before using them in the simulation, are:

- Routing Protocol
- Authentication Time Interval (ATI)

6.4.1.3 Parameter Values

The parameter values used in the NS-2 based evaluation have been discussed in Chapter 5. **Table 6.1** provides a summary of these simulation parameters.

There are other parameters that need to be set while performing the experiments. These parameters play an important role in ACM-MANoN, Authentication Time Interval (ATI) of the digital certificates, number of PKIs, and the number of CA in each PKI.

Choosing the values of these parameters will be a trade-off between ACM-MANoN's performance and its communication cost, as will be shown in the next section.

The values chosen for these parameters in running the experiments are 1 second for ATI, 4 for the number of PKIs, and minimum number to apply threshold cryptography of 4 CAs (3 CA_{Se} and $1CA_{C}$). The selection of these values is justified in the following section.

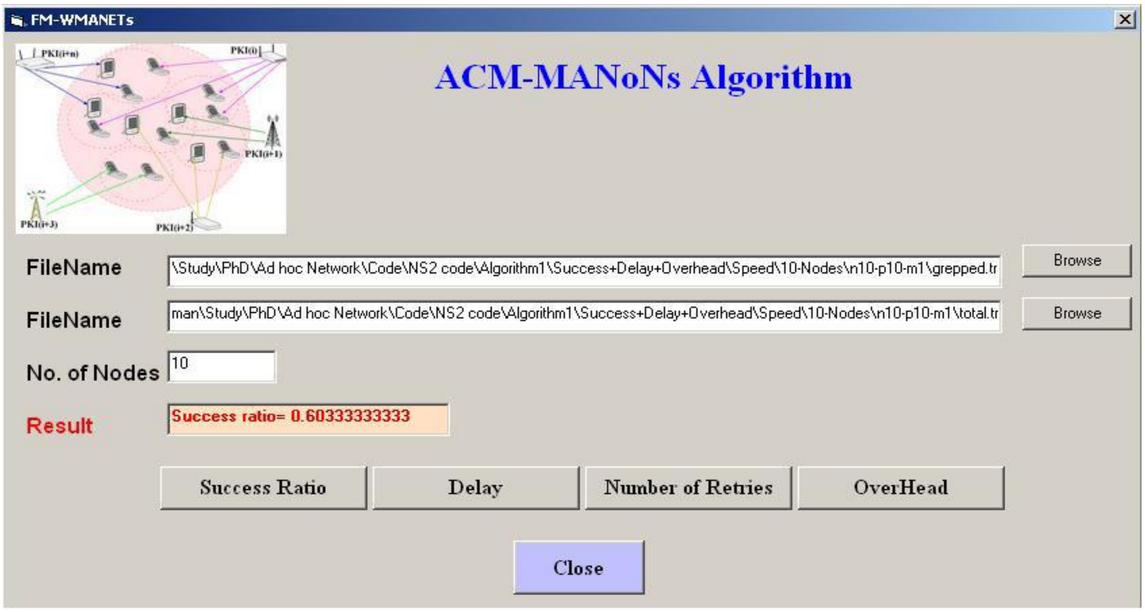
Scenario Name	*Mobility (Pause Time) Scenario*	*Max Node Speed Scenario*	*Network Size Scenario*
Pause Time (s)	0, 10, 40, 60, 100	10	10
Max Node Speed (M/s)	20	1, 10, 15, 20, 25, 30	20
Number of Mobile Nodes	50	50	10, 20, 40, 60
Simulation Time (s)	500	500	500
Network Space (m)	1000 x 1000	1000 x 1000	1000 x 1000
Radio Range	250m	250m	250m
MAC Protocol	IEEE 802.11	IEEE802.11	IEEE802.11
Radio Propagation Model	two-ray	two-ray	two-ray
Antenna Model	Omni Antenna	Omni Antenna	Omni Antenna

Table 6.1: The parameter values used in NS-2 based simulation

6.4.1.4 Results and Analysis

As mentioned earlier, each result presented in this section is achieved by averaging 30 runs. The corresponding traces files, after a filtering process, were sent to a Visual Basic tool, which is developed in order to measure the different metrics as shown in Figure 6.6.

The performance of ACM-MANoN, in terms of success ratio, delay, overhead and number of retries could be much affected by other factors such as ATI and routing protocols. In order to choose proper values for these factors, to be used throughout the simulation, a set of experiments were executed. The results of these experiments are shown in Figures (6.7 - 6.11).



FileName \Study\PhD\Ad hoc Network\Code\NS2 code\Algorithm1\Success+Delay+Overhead\Speed\10-Nodes\n10-p10-m1\grepped.tr

FileName man\Study\PhD\Ad hoc Network\Code\NS2 code\Algorithm1\Success+Delay+Overhead\Speed\10-Nodes\n10-p10-m1\total.tr

No. of Nodes 10

Result Success ratio= 0.60333333333

Figure 6.6: Visual Basic tool used to measure the evaluation metrics of MANoN

As can be seen in Figure 6.7, changing the value of ATI (the time interval between two consecutive retries) mainly affects the delay. As the value of ATI increases, so does the delay. Meanwhile, the success ratio and average number of retries remain almost unchanged. Figure 6.8 illustrates the slight increase of overhead due to decreasing ATI. Based on these observations, the value of ATI used in the experiments was 1 second.

The average delay metric is measured in the simulation in the following way:

Delay (simulated) = certificate authentication (***END***) – certificate authentication (***START***)

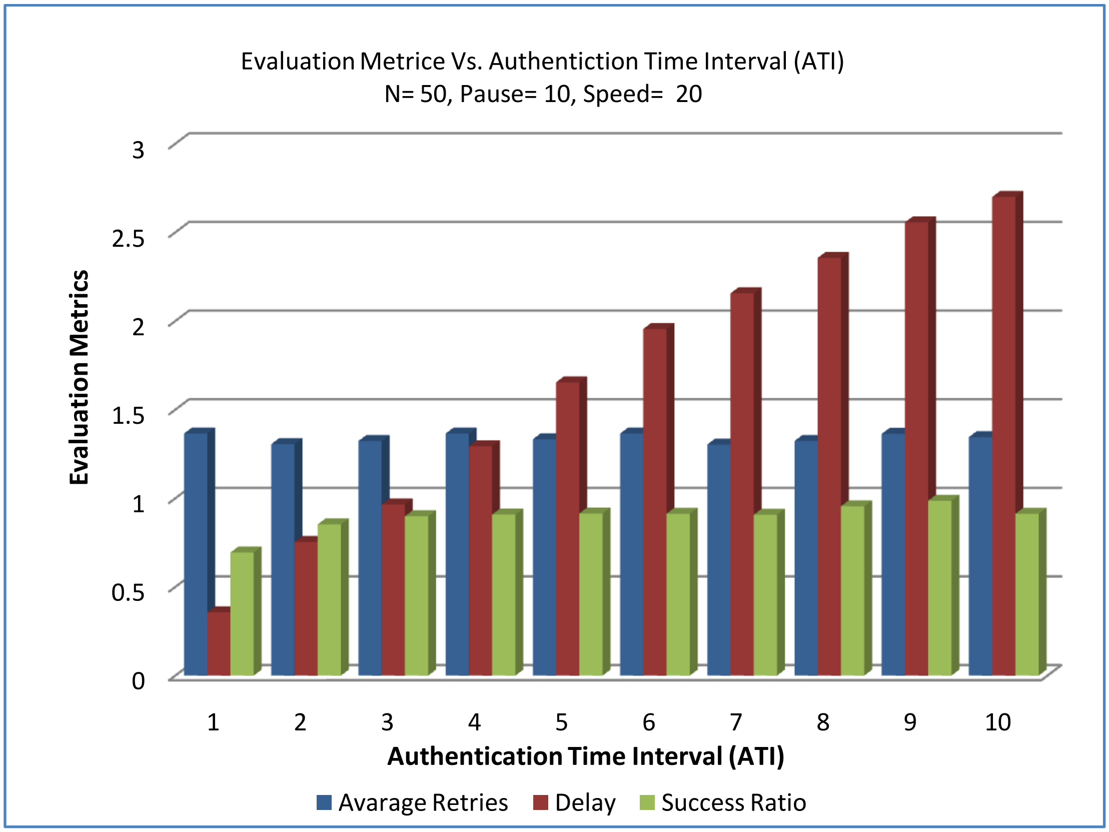


Figure 6.7: Success ratio, Delay, and Average Retries versus ATI

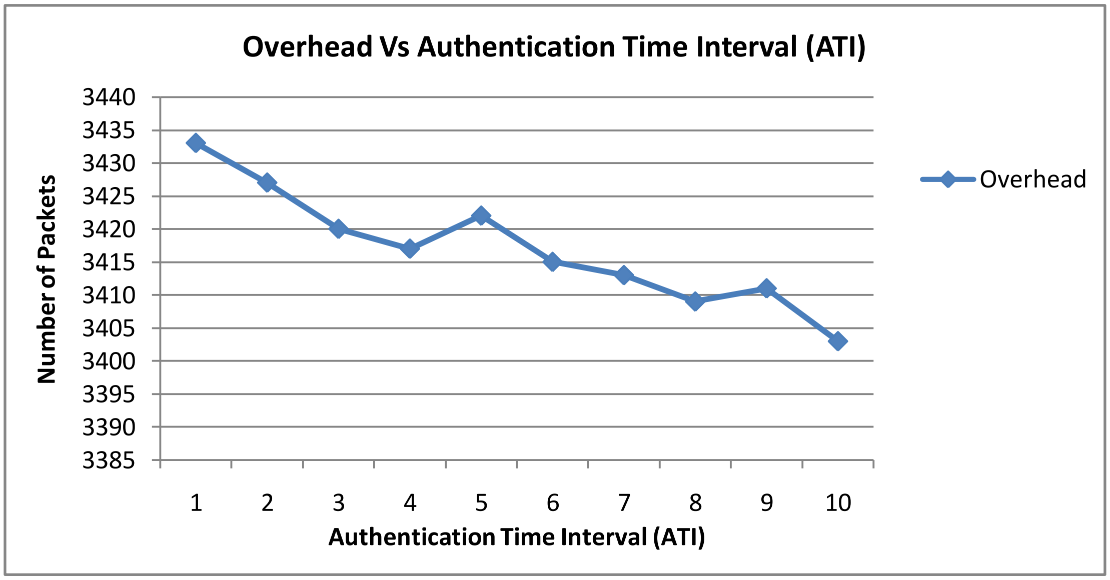


Figure 6.8: Overhead versus ATI

When studying the impact of ATI on the average delay of the certificate authentication ACM-MANoN, that average delay can be calculated using the following formula:

Delay (calculated) = (ATI * Number of Retries) - ATI

Figure 6.9 shows a comparison between the simulated average delay and the calculated average delay. It can be observed from this comparison that the calculated average delay almost matches the simulated average delay.

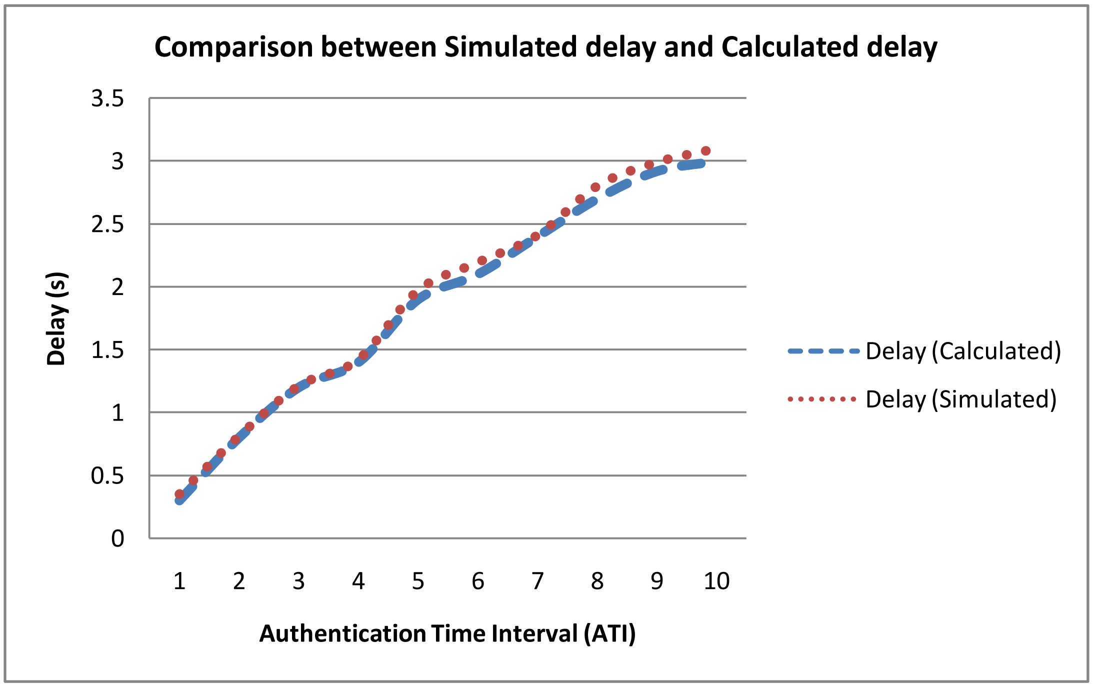


Figure 6.9: Comparison between the simulated and calculated delays

A set of routing protocols including Ad hoc On-demand Distance Vector (AODV) [91], Destination Sequence Distance Vector (DSDV) [92] and Dynamic Source Routing (DSR) [61] is implemented by NS-2. The routing protocol used in all experiments conducted in the present study was AODV, which was chosen as the result of a study for all the evaluation metrics used to test ACM-MANoN performance. The results of this study are shown in Figure 6.10 and Figure 6.11.

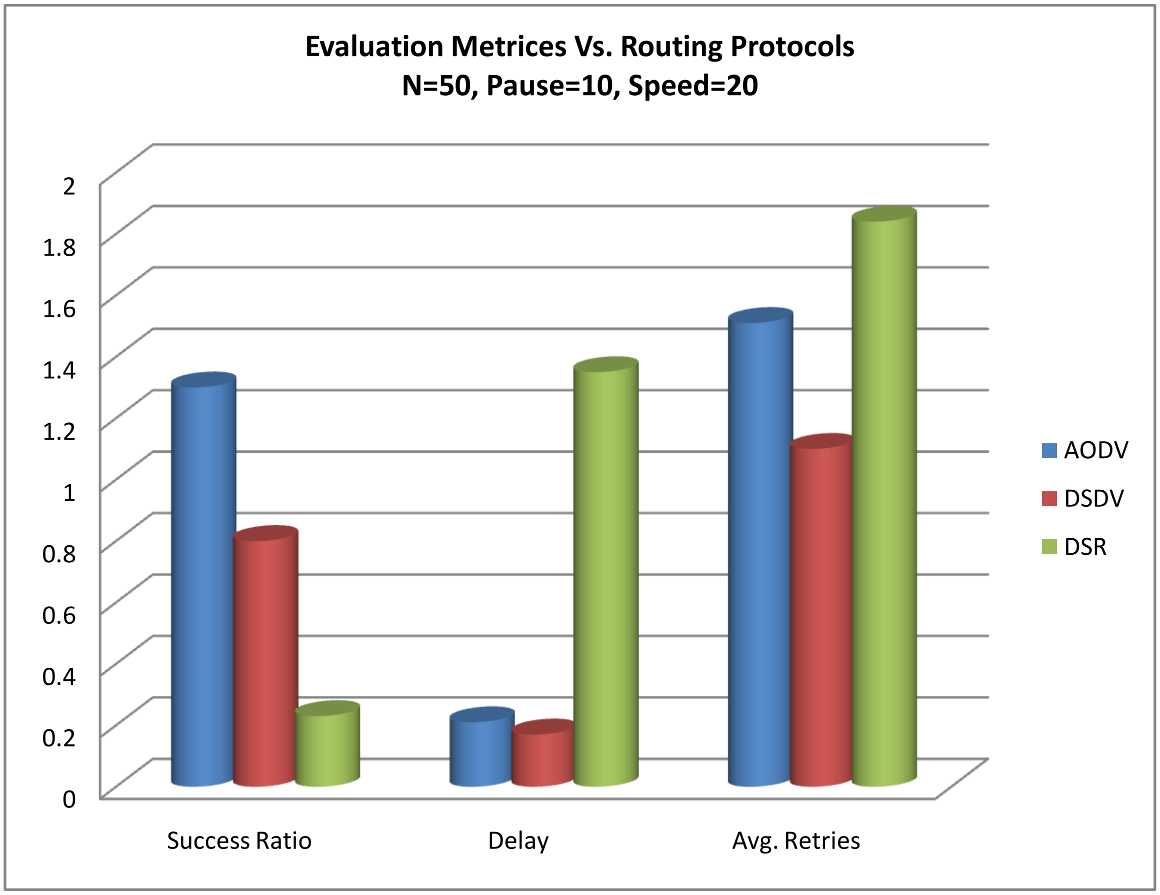


Figure 6.10: Success Ratio, delay and average retries versus routing protocol

AODV gives the best success ratio, with a little more delay and average number of retries than DSDV. DSDV gives the lowest delay and average number of retries, but presents a problem regarding the large amount of overhead it causes in ACM-MANoN (Figure 6.11).

In contrast, DSR is the best routing protocol regarding the overhead but conversely the worst regarding the success ratio, delay and average number of retries. All in all, AODV was the best routing protocol to use in the experiments.

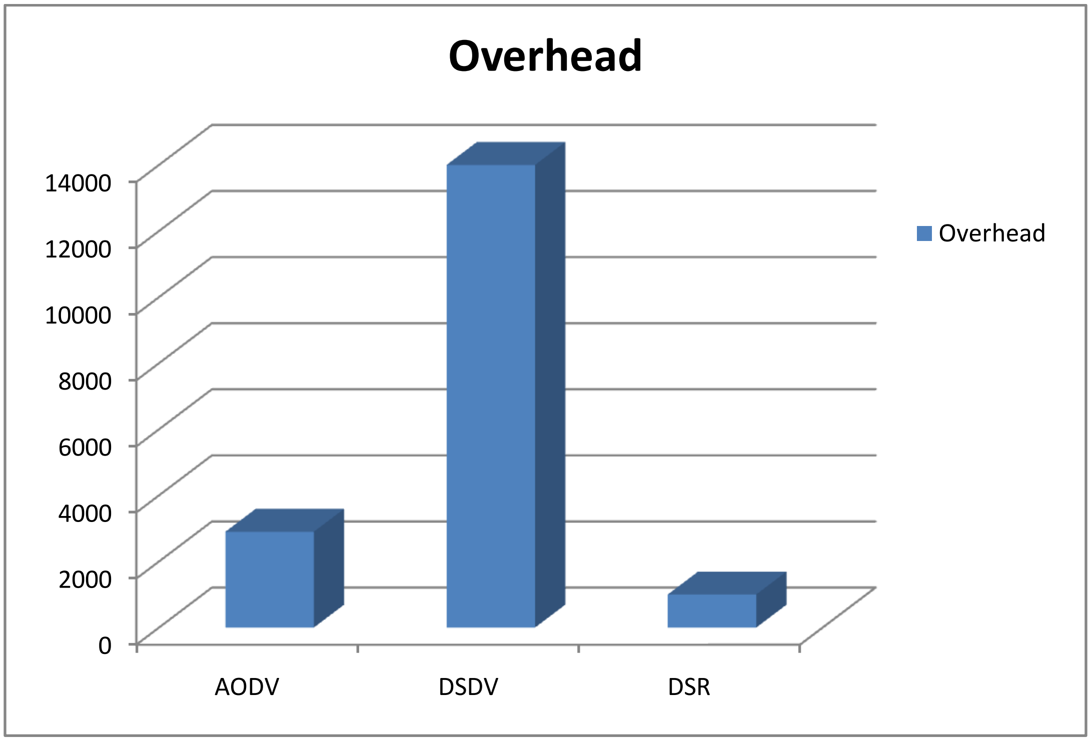


Figure 6.11: Overhead versus routing protocols

6.4.1.4.1 Success Ratio

The **Figures (6.12-6.14)** will show the success ratio versus the three different scenarios of mobility, speed and network size. As mentioned before, the success ratio measures the number of successful certificate authentication requests to the total number of certificate authentication requests that take place during the simulation time in addition to the authorisation certificate.

It is assumed that each node will make at least one authentication request. Therefore, the total number of authentication requests made during the simulation time is equal to the number of nodes trying to enter the MANET.

It is worth mentioning that the maximum number of retries the security protocol permits affects the success ratio in these three scenarios. Therefore, a study has been done to help determine the optimum maximum number of retries that need to be set in our experiments. Figure 6.12 shows that the success ratio, delay and overhead of ACM-MANoN increase with the number of retries. Three retries have been chosen in testing the performance of ACM-MANoN. This is because after 3 retries there is not a noticeable increase in the success ratio, while the delay and overhead continue to increase.

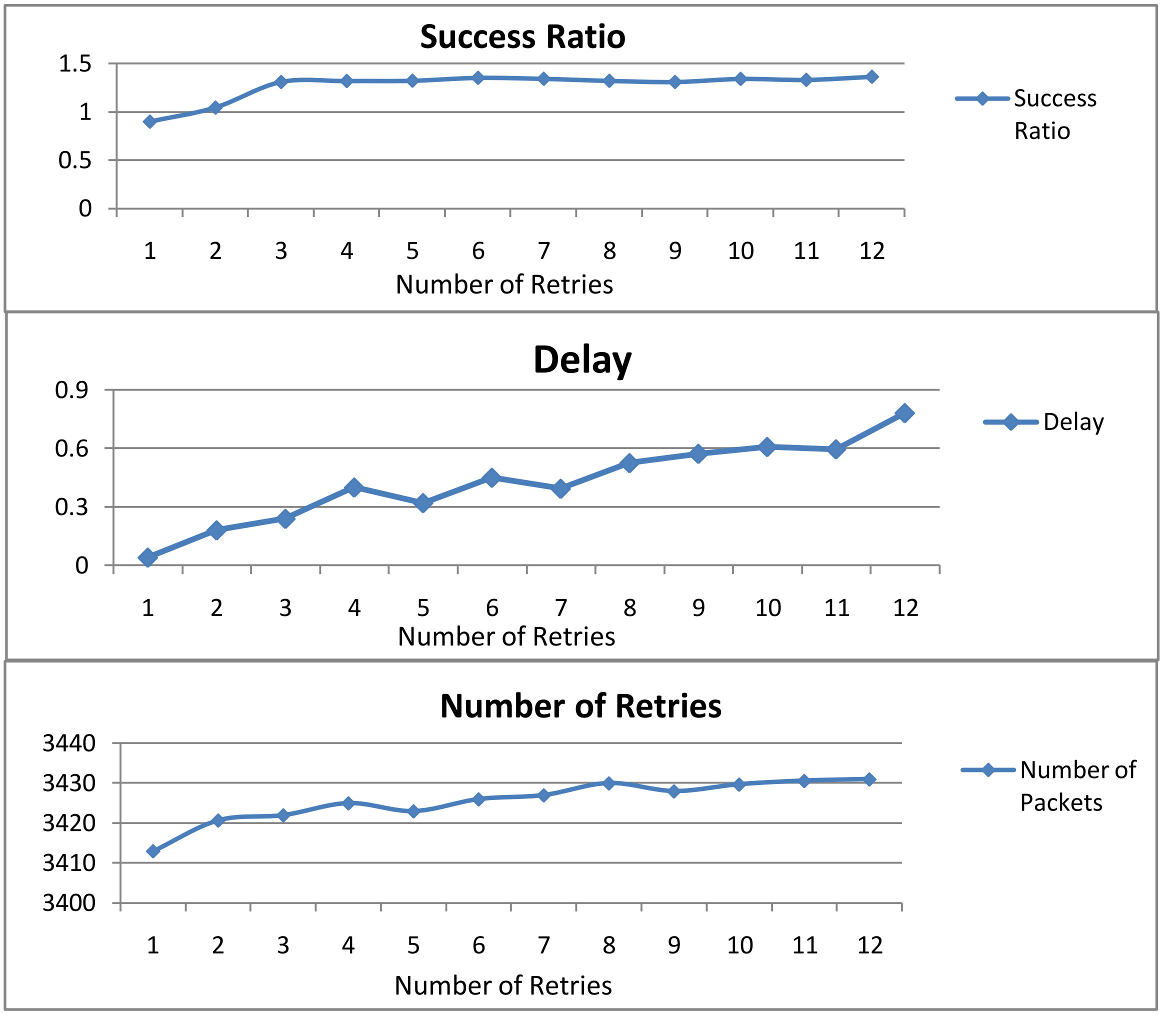


Figure 6.12: Success Ratio, delay and Number of Packet versus number of retries

Figure 6.13 shows the success ratio against mobility and network size. Mobility is most often a big issue in developing ad hoc protocols. As can be seen, ACM-MANoN is not much affected by mobility. In general, the success ratio increases with high mobility situations and large network sizes.

Moreover, the effect of mobility is more noticeable with a small number of nodes, especially if that number falls below 30. This is due to the number of neighbour nodes. The number of neighbour nodes based on transmission range and simulation area can be calculated using the formula

$$\frac{(\pi \times r^2)}{\left[\frac{w \times h}{n}\right]}$$

Where w = area width, h = area height, r = transmission range, n = number of nodes [65].

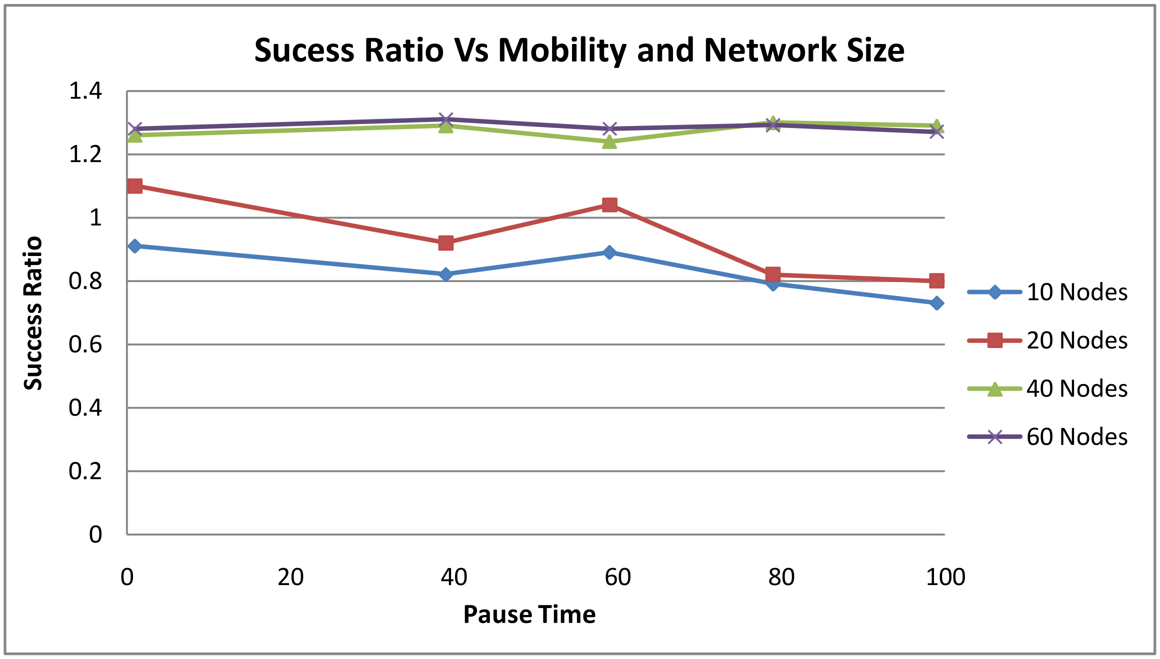


Figure 6.13: Success Ratio versus mobility and network size

For example, when the network size is 10, the number of neighbours is around 1.96, but when the network size is 30 the number of neighbours is more than 6. Therefore, the effect of mobility increases with a lesser number of nodes, because high mobility reduces the effect of fewer neighbourhoods.

Figure 6.14 shows the success ratio against speed and network size. The ACM-MANoN is not strongly affected by speed, but in general, as speed increases so does the success ratio. The influence of speed is more noticeable with small network sizes in a manner similar to that of mobility. ACM-MANoNs provide a better success ratio in large network sizes.

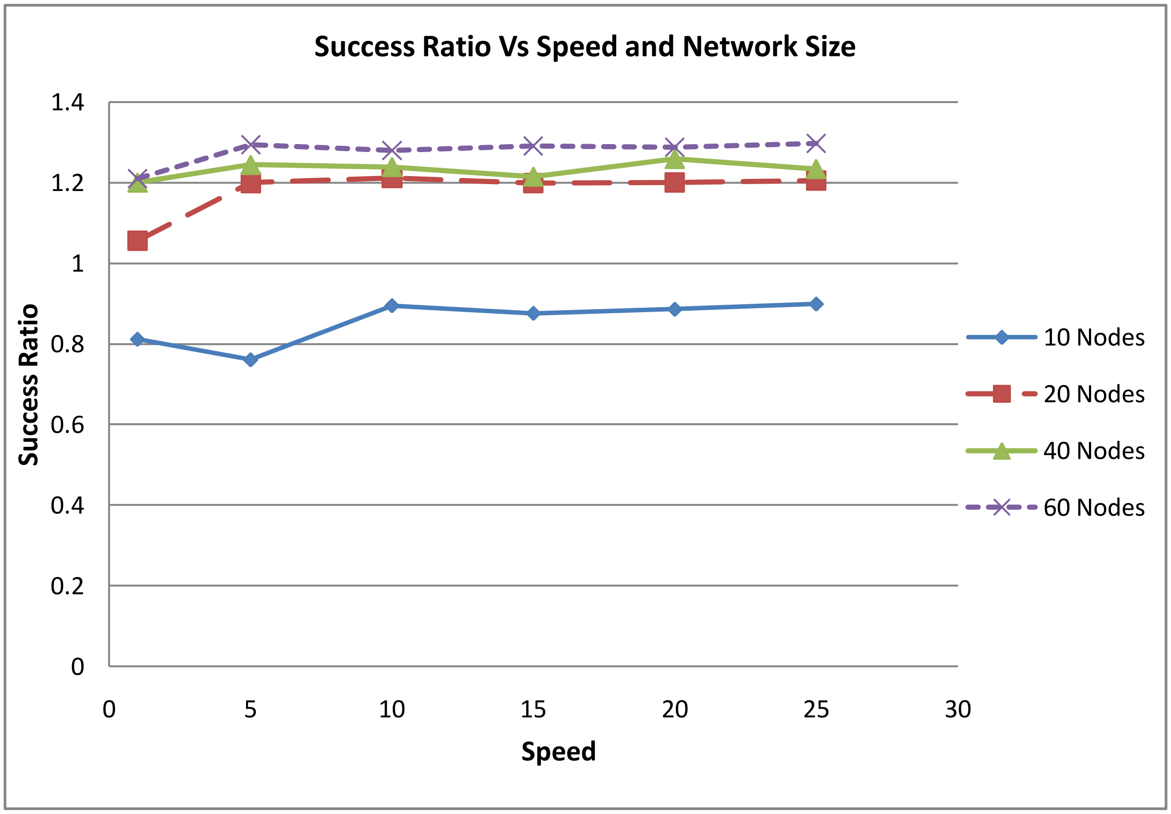


Figure 6.14: Success Ratio versus speed and network size

6.4.1.4.2 Delay

Figures 6.15 and 6.16 show the average delay versus mobility, speed and network size. As mentioned before, the average delay metric measures the average time taken to successfully authenticate a certificate and issue an authorisation certificate.

Regarding mobility, the average delay reduces by decreasing the pause time as shown in Figure 6.15. In addition, large network size leads to an increase in average delay. Increasing network size will increase the communication load, resulting in a longer wait in the links' queues, more dropping of packets and a greater number of retries, all of which consequently causes more delay. The queue size used in the experiments was 50 packets. A network size greater than 20 nodes will cause a correspondingly greater delay than will be the case with a smaller network.

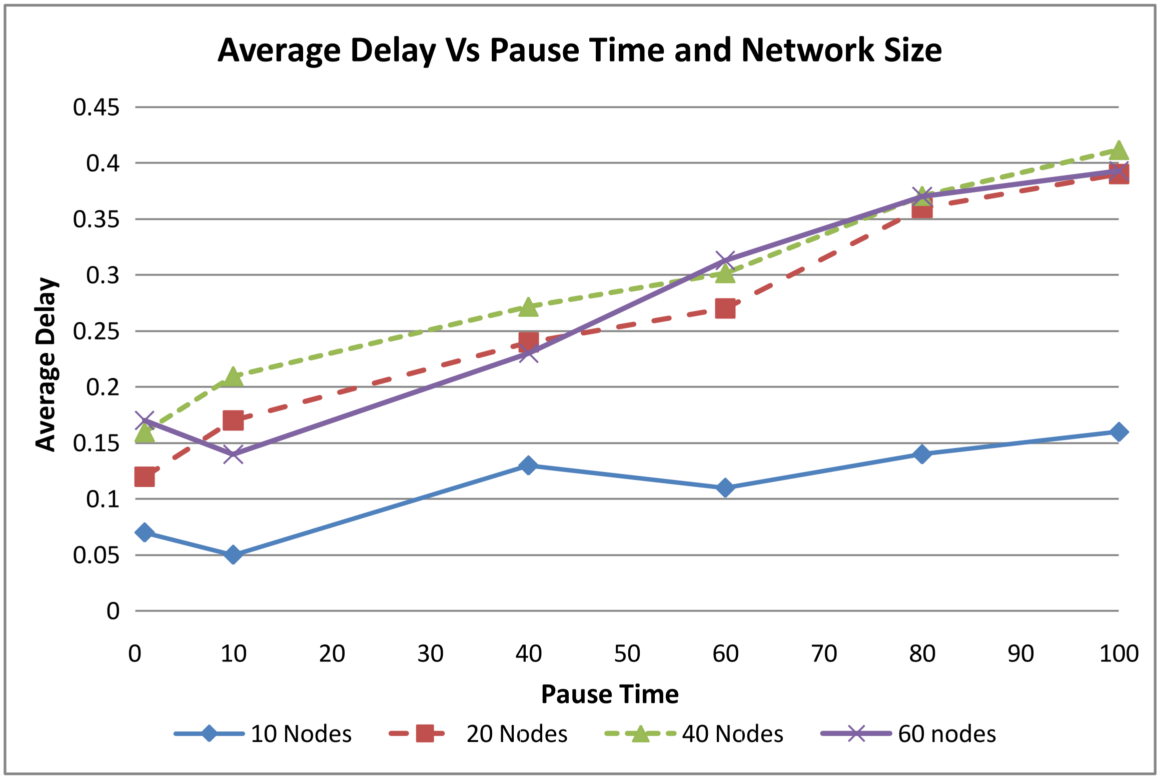


Figure 6.15: Average delay versus mobility and network size

As speed increases, average delay decreases as shown in Figure 6.16. Also, the average delay in networks smaller than 20 nodes was lower than that in larger networks.

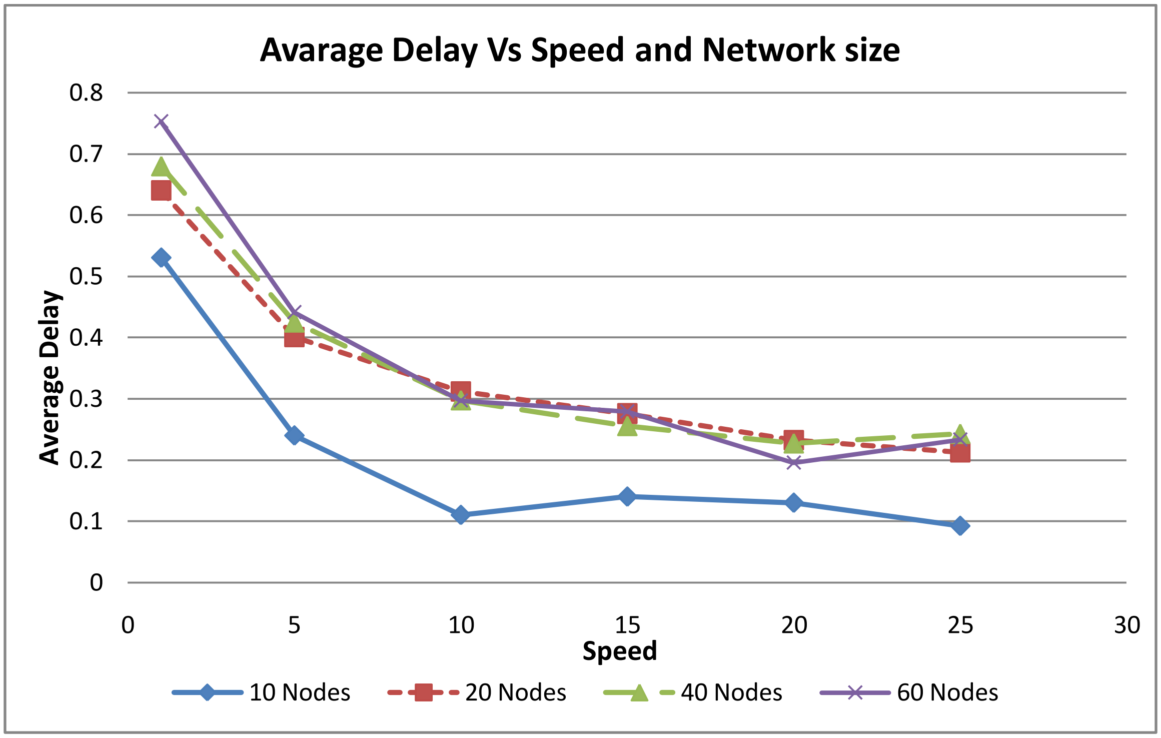


Figure 6.16: Average delay versus speed and network size

6.4.1.4.3 Overhead

Figures 6.17 and 6.18 demonstrate ACM-MANoN overhead in terms of the number of packets generated by this security protocol. There are three types of packets in ACM-MANoN algorithm: *certificate packets*, *request packets* and *reply packets*. For the MANoN with *N* nodes, the total number of generated packets is equal to the number of certificate packets, the number of request packets *(Max(N))* and the number of reply packets *(Max(N))*.

This explains why the overhead is almost unchanged for the same number of nodes (Figure 6.17 and 6.18). The overhead has been calculated against the network mobility, speed and size. As mobility decreases the overhead increases slightly, especially when network size is greater than 10 nodes, as depicted in Figure 6.17. It is also obvious from this figure that overhead increases with an increase in network size.

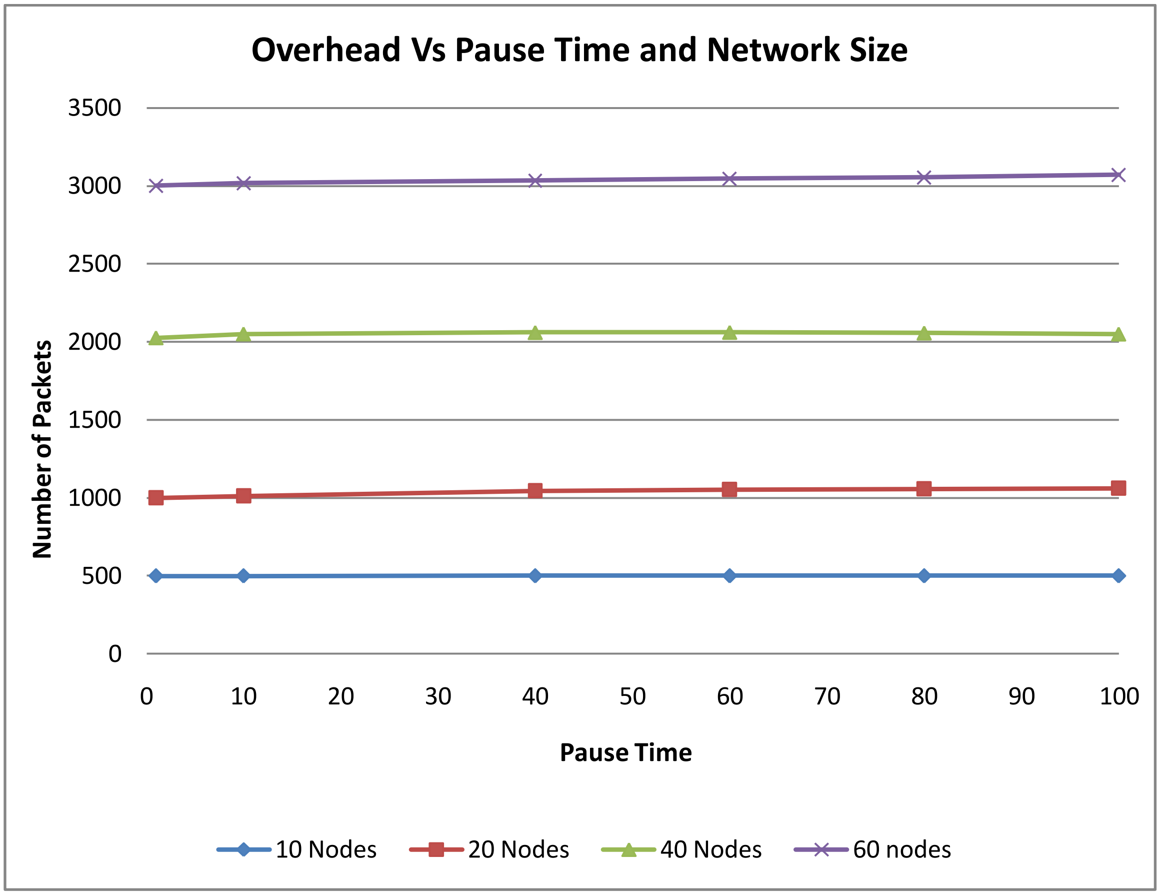


Figure 6.17: Overhead versus mobility and network size

As the nodes speed increases, it can be observed that the overhead remains almost unchanged for ACM-MANoN (Figure 6.18); the overhead slightly decreases when the speed increases. Figure 6.18 illustrates the increase in overhead caused by increasing network size.

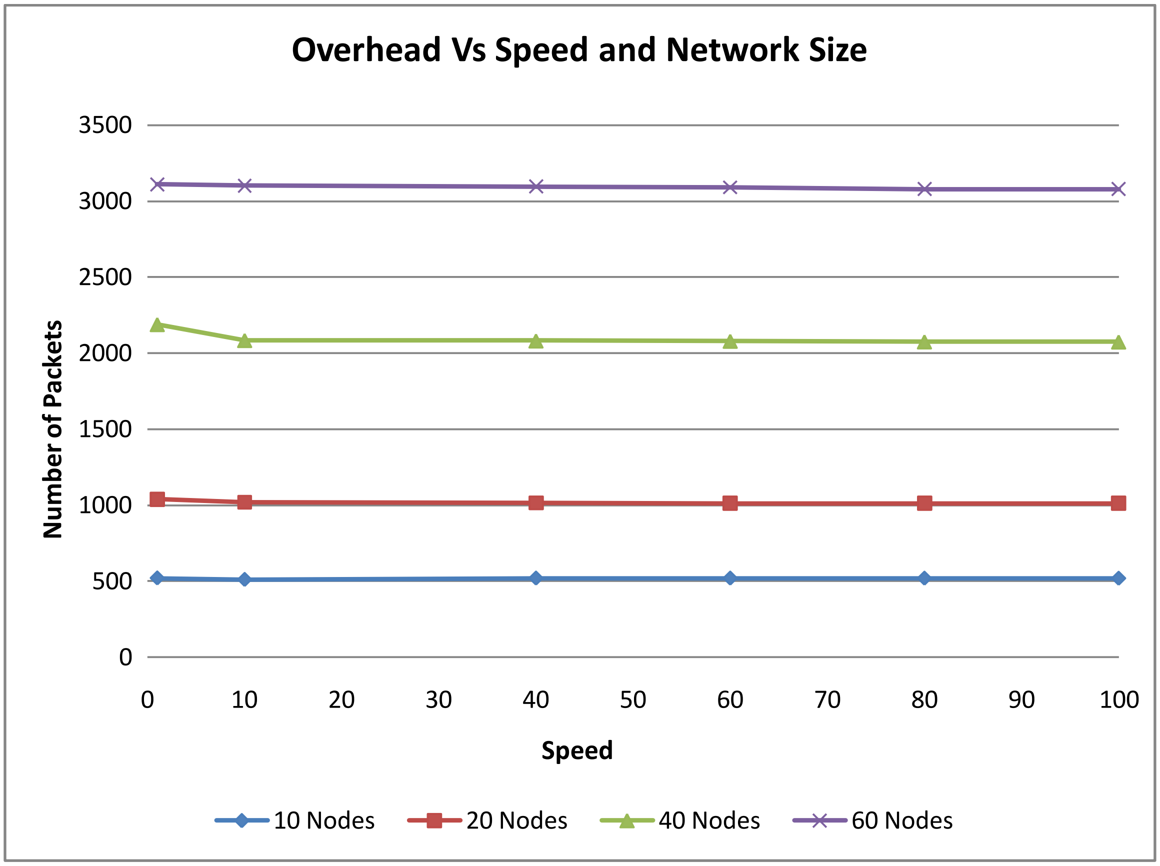


Figure 6.18: Overhead versus speed and network size

6.4.1.4.4 Average Number of Retries

The average number of retries metric, which measures the average number of retries before a node successfully authenticates a certificate, has been calculated against three different scenarios mobility, speed and network size. The results of these studies are shown in Figures 6.19 and 6.20.

In general, the average number of retries increases as the mobility and speed decrease, as can be seen in Figures 6.19 and 6.20. It can be also observed in these two figures that the average number of retries is not enormously influenced by network size.

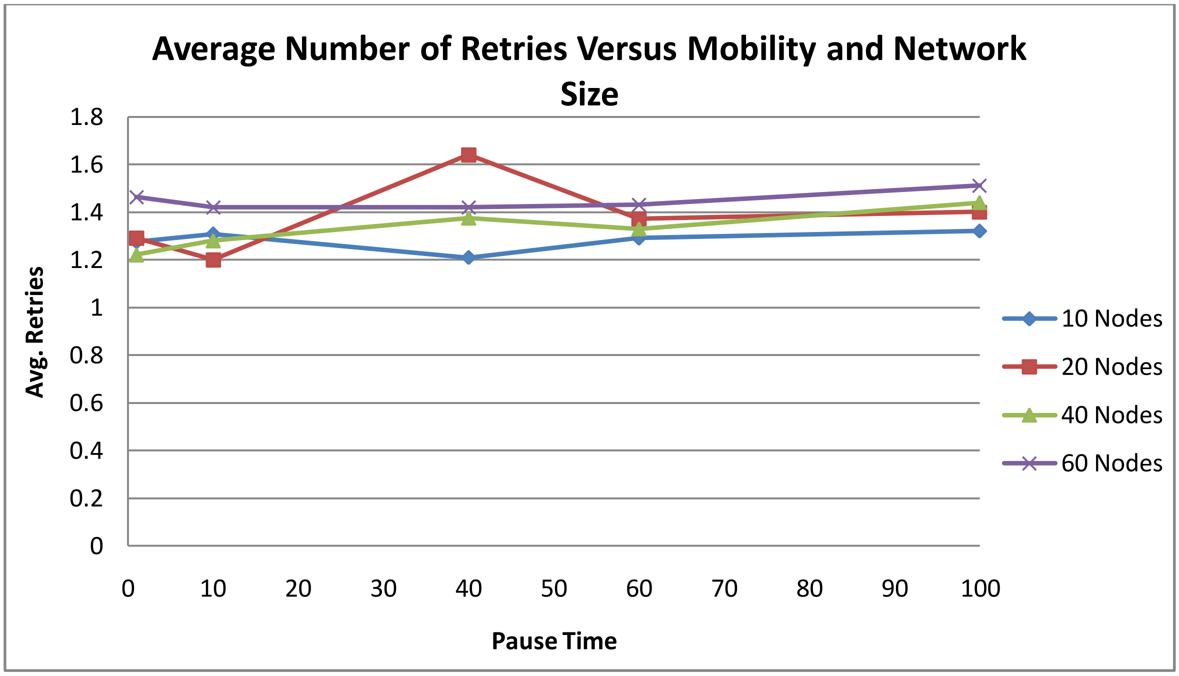


Figure 6.19: Average number of retries versus mobility and network size

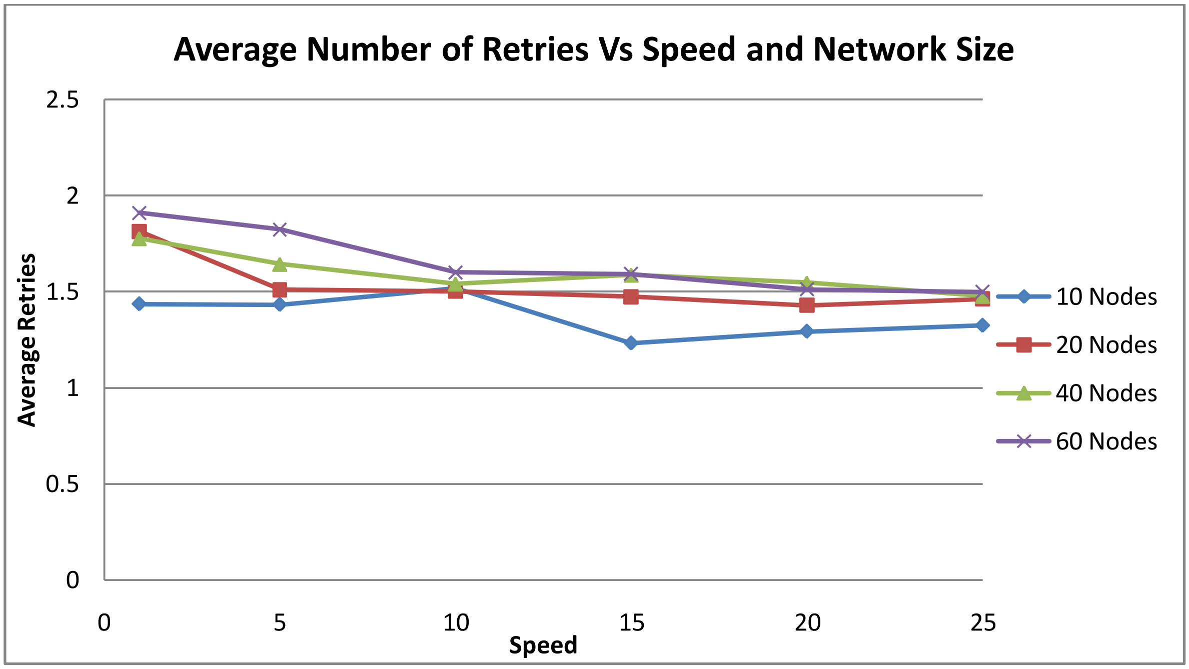


Figure 6.20: Average number of retries versus speed and network size

As we know that it is impossible to simulate all the possible situations that could take place in the real world, we can not exactly predict how any security protocol is going to behave. However, the results shown above give, to some extent, a clear idea of how ACM-MANoN is going to perform in real network environments.

ACM-MANoN has been simulated in different scenarios with different parameter values. The selection of these parameter values has been justified. In real applications of ACM-MANoN, these values could be selected based on the business requirements of the applications themselves. Consequently, a higher priority could be given to some evaluation metrics than to others. That will certainly affect the choice of these parameter values.

6.5 Discussion

Sections 6.2 to 6.3 have presented the ACM-MANoN algorithm. In section 5.4 the evaluation of ACM-MANoN has been shown and analysed. However, attention should be drawn to some important issues, including ACM-MANoN applications, ACM-MANoN security attacks and ACM-MANoN certificates. These issues will be discussed in the following sections.

6.5.1 ACM-MANoN Applications

This section presents examples of ACM-MANoN applications in the military and civilian environments. An example of ACM-MANoN for military use is shown in Figure 6.21. NATO [82] was used to show how ACM-MANoN could be applied effectively in such environments. NATO provides a forum in which the United States, Canada and European countries can consult together on security issues of common concern. If these countries are located in a battlefield representing a MANoN space, each one of them should have a PKI to ensure secure communications between the members of their networks. Since these countries collaborate, they could agree to distribute their CAs' public keys. Under these circumstances, ACM-MANoN will very securely authenticate certificates belonging to the same or different CAs (more explanation will be provided in chapter 8).

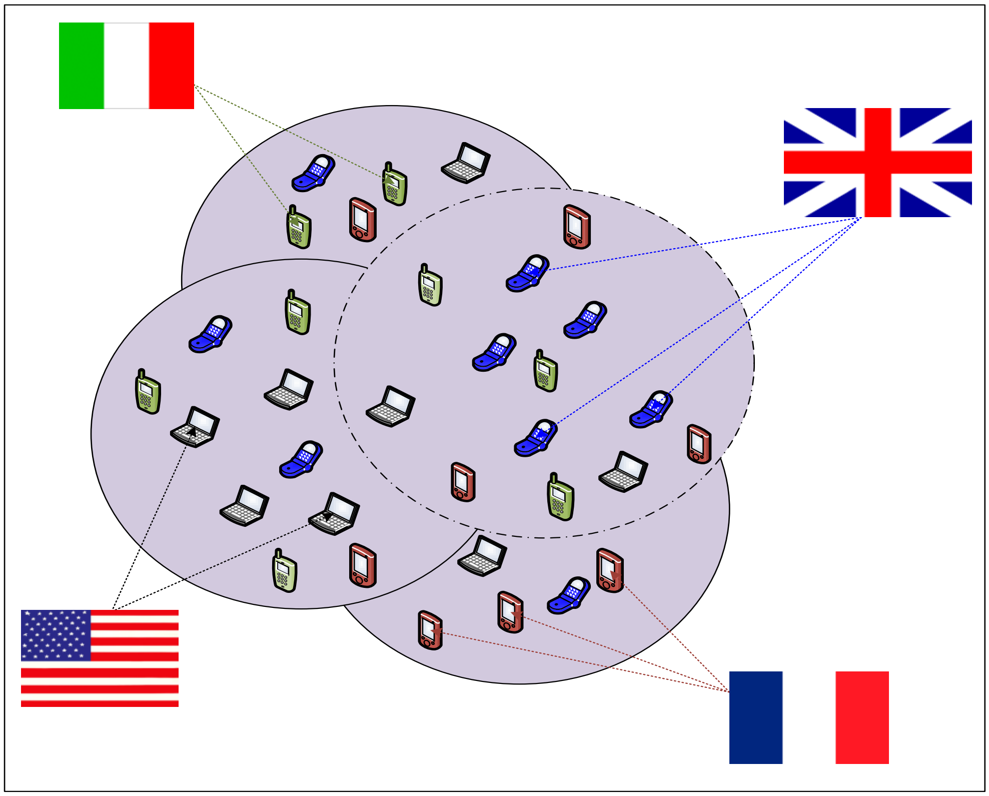


Figure 6.21: Military Applications for the ACM-MANoN

An example of applying ACM-MANoN in the ***civilian environment*** is shown in Figure 6.22. If an area like Leicester town centre is chosen to represent the network space of MANoN, then the set of possible infrastructure-based wireless networks that could co-exist are the mobile operators known in this area such as Orange, O_2, Three and Vodafone.

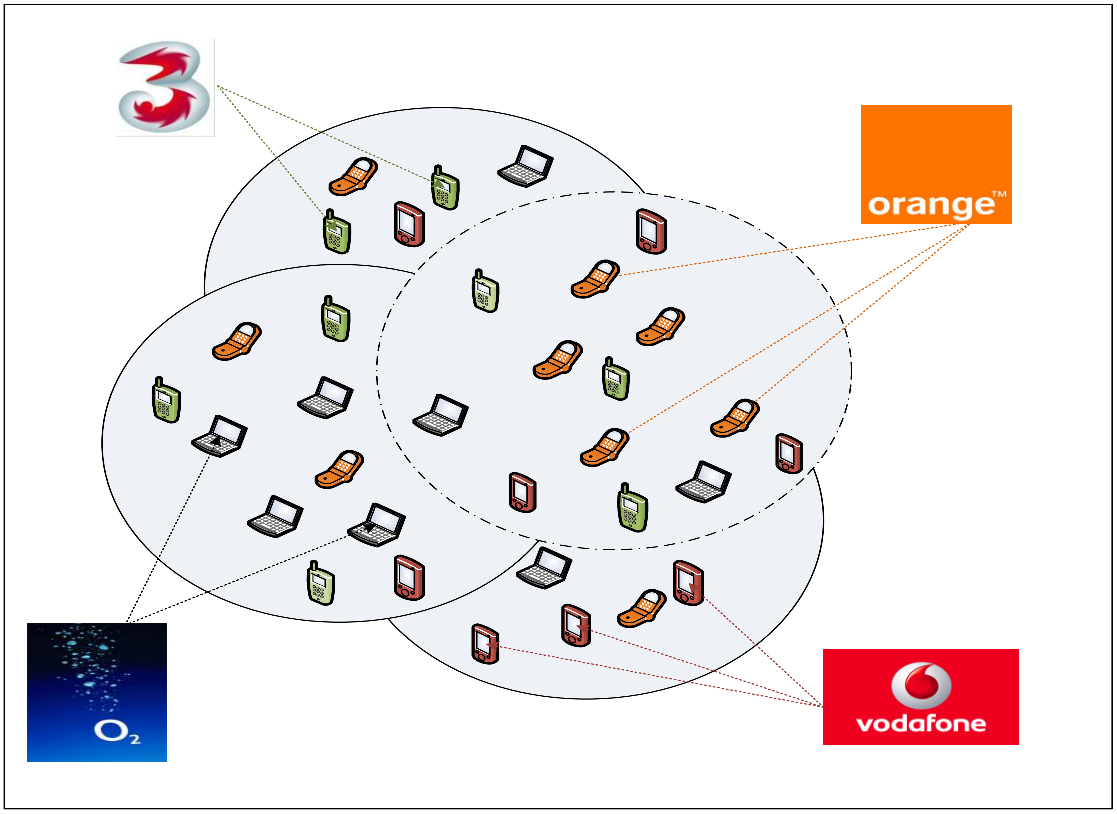


Figure: 6.22 Civilian applications of ACM-MANoN algorithm

6.5.2 ACM-MANoN Security Attacks

Before trying to classify the different attacks that the ACM-MANoN algorithm might be subjected to, it is important to understand fully their behaviour and to ascertain if they are really causing any damage to the service provided by ACM-MANoN.

In the case of a misbehaving node, which has created a fake identity with a fake digital certificate, this type of behaviour is non-harmful as all public keys of the system are installed in the Local Data Base (LDB) of the CAs, so when the comparison is made with the LDB, public key will not be known and the node will not gain authorisation certificate to perform in the system, if this identity is not for any other honest ad hoc node this misbehaving action has no impact on the MANoN.

6.5.3 ACM-MANoN Certificates

This section considers various subjects related to ACM-MANoN certificates, such as the formatting, and revocation processes.

- **Certificate format:** The main structure of ACM-MANoN's digital certificates is presented in section 6.3.1. Even though these certificates are issued by different PKIs, there should be a common structure for the digital certificates used by all them. This can be achieved by following the certificate format defined by ITU-T in its recommendation X.509 [54].

- **Certificate revocation:** If certificate renewal is the responsibility of MANoN nodes, there will be no guarantee that nodes will collaborate to keep track of the revocation process in an honest, effective manner. This is a strong advantage of the ACM-MANoN algorithm: it pushes the revocation process based on the existing infrastructure regardless of whether or not the node cooperates.

6.6 Summary

A novel access control mechanism security protocol for managing digital certificates in MANoN called ACM-MANoN is proposed. This protocol assumes that all MANoN nodes are part of other infrastructure-based wireless networks.

Using a small amount of information from these wireless networks has provided a big improvement in managing the digital certificates. The trust model used by ACM-MANoN is a heterogeneous hierarchical one. Each of the existing wireless networks has a minimum number of four professional CAs of servers and combiners belonging to PKI network. The CA issues digital certificates for the nodes belonging to its network and other networks.

ACM-MANoN deals with threshold cryptography as it is the key management service with a high level of security, CAs applied in previous research lack this high security demand such as cluster head (CH) [64, 29].

This security mechanism provides a ***highly secure*** prevention technique. It supplies MANoN with digital certificates issued by professional CAs. Other approaches regarding security management have serious shortcomings regarding the level of security achieved, assumptions taken and the total computation and communication costs, as discussed in Chapter 2. In addition, ACM-MANoN improves the ***availability*** of the key management service in MANoN. This is due to the support given by existing infrastructure-based wireless networks.

Availability has been shown in the results in terms of delay and the average number of retries. The maximum delay recorded in all experiments in all scenarios was less than 0.9 seconds. In all the results recorded, the average number of retries was less than 2. It can thus be shown that ACM-MANoN constitutes a highly available key management service to MANoN.

An interesting observation resulting from the experiments intended to test the impact of the network size on the performance of ACM-MANoN is that this security protocol is ***scalable***. ACM-MANoN provides high success ratios with large networks.

Both delay and average number of retries rose only with an increase in network size. There was an increase in overhead, in terms of the number of packets transferred in the network (certificate, request and reply packets), with an increase in network size.

ACM-MANoN could be successfully applied in different scenarios and applications. It offers ***flexibility*** in different ways. There are no constraints or conditions on the application of ACM-MANoN except the network model, which assumes that MANoN operates in heterogeneous wireless networks and MANoN nodes are managed simultaneously by these wireless networks.

As shown by the experimental results, ACM-MANoN has performed well with different numbers of PKI, network size, pause times and speeds. Based on the evaluation metrics used to test the performance of ACM-MANoN including success ratio, delay, number of retries and overhead, the results of NS-2 studies demonstrate an ***efficient*** management service provided by ACM-MANoN.

ACM-MANoN is evaluated using the NS-2 simulator. The results of the evaluation confirm that ACM-MANoN is a ***fully distributed*** security protocol that provides ***a high level of secure, available, scalable, flexible and efficient*** key management services for MANoN. It is obvious that ACM-MANoN is a ***fully distributed*** security protocol. It depends on number of CA in our MANoN called (servers and combiners), which are responsible of managing and validating digital certificates of MANoN nodes.

Applications of ACM-MANoN in civilian and military environments have also been discussed. Various issues regarding ACM-MANoN such as simulation methodology, certificate structure, and certificate revocation have been explored.

Chapter 7

Detection Algorithm for MANoN

Objectives

- Defining our detection component for MANoN
- Implementing our BD-MANoN
- Designing an architecture framework for our BD-MANoN
- Describing our BD-MANoN in formal description method
- Dealing with attacks in the BD-MANoN

7.1 Introduction

The integration of heterogeneous wireless technologies can improve network performance, thereby meeting different security requirements, as will be shown in this Chapter. The research into integrating MANoN with other wireless networks such as cellular networks can be found in [71, 116]. These focus on how MANoN can enhance cellular services.

This chapter provides a novel behavioural detection algorithm BD-MANoN for managing certificates, and on order to fulfil detection security management requirements. BD algorithm is based on the behaviour of nodes'; to achieve this detection, a set of BBN will carry out the observations in order to differentiate between malicious and normal nodes in the MANoN.

The following sections present the network and system model constituting the basis of BD-MANoN. The BD-MANoN certificate management framework is defined and the means of coping with misbehaving nodes in this algorithm is explained. Finally, this algorithm will be evaluated using several case studies.

7.2 Network Design and System Model

In the BD-MANoN algorithm, some of the ad hoc nodes are involved in other infrastructure-based wireless networks such as WLAN and cellular systems, and will therefore belong to their PKIs creating the MANoN system, as shown in Figure 7.1.
Other non-managed MANET nodes which are not involved in any other wireless networks will be observed by our detector nodes (BBN) in order for those undefined nodes to be able to gain access to our MANoN system, as will be shown in the following sections.

Similar to our ACM-MANoN algorithm in the previous chapter, our MANoN will consist of a number of MANETs interconnecting with each other. Nodes in our MANoN will be classified thus: *General Nodes (GN)* i.e. regular ground nodes are typically soldiers equipped with communication and computation limited devices, and *Back-Bone Nodes (BBN)* are usually special units, such as tanks and personnel carriers, which have more extensive facilities than regular ground nodes. BBN nodes can establish direct wireless links for communication amongst themselves. This type of node will carry out the CA (Servers CA_{Se} and Combiners CA_{C}) duty signing and creating new certificates for different nodes in the MANoN system.

It is assumed that all wireless transmission links in this network are bidirectional. Moreover, two kinds of network cards will be presented. The first is a GN with an ad hoc network card. The second is BBN that possesses both one ad hoc network card and one heterogeneous network card; BBN can communicate with neighbourhood nodes and other heterogeneous networks (such as satellite, unmanned aerial vehicle, or cellular networks). In this system environment, we assume that there exists a wide area covered heterogeneous network such as satellite, unmanned aerial vehicle or cellular networks, as depicted in Figure 7.2. The wide area covered heterogeneous network can connect with the internet. Moreover, its service area is fully covered with a large place (e.g. island of Bahrain) or super machines (servers).

In addition, some PKIs are pre-connected by wireless connection to exchange data and update information. Each PKI has a set of *t+1* CAs acting as administrators; those CAs are *fully* trusted by all nodes that belong to this PKI. It is relatively uncommon to have one node that belongs to more than one PKI, because this protocol is used either in civilian environments or military environments where the number of PKIs within a given area is limited.

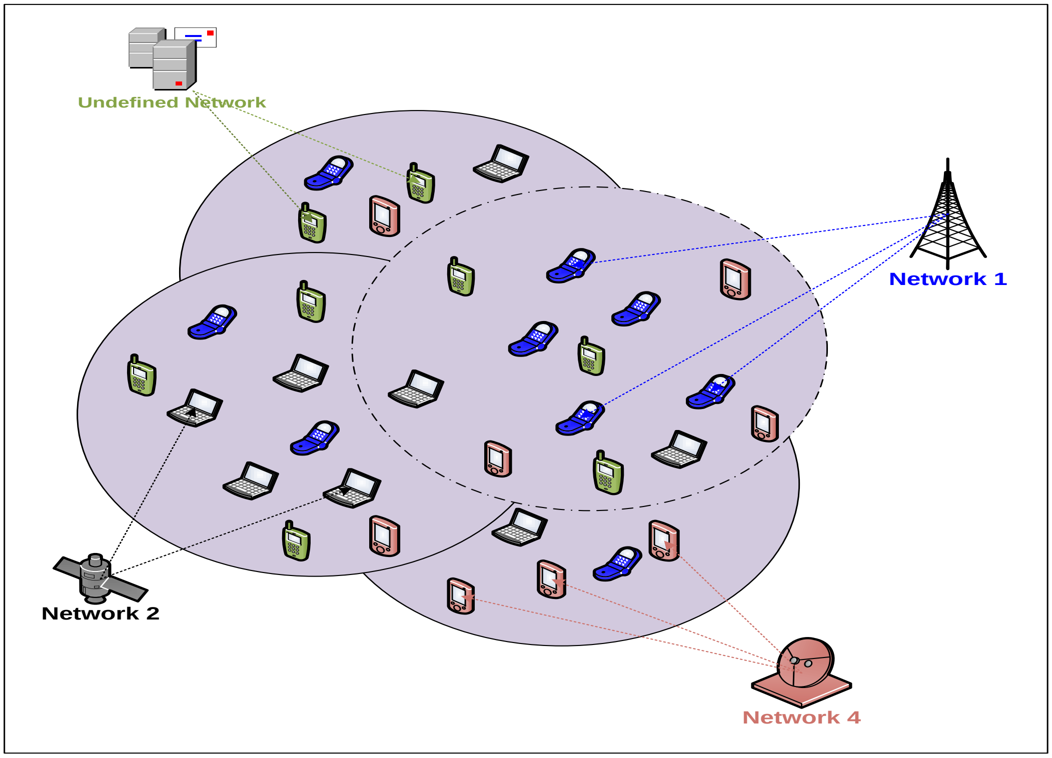


Figure 7.1: Network Model of BD-MANoNs

This will include the PKIs of the known mobile operators and wireless LANs in that area. For example, there is no common node that belongs to both mobile operators Orange and O_2, or two nodes that belong to both the UK and US armies.

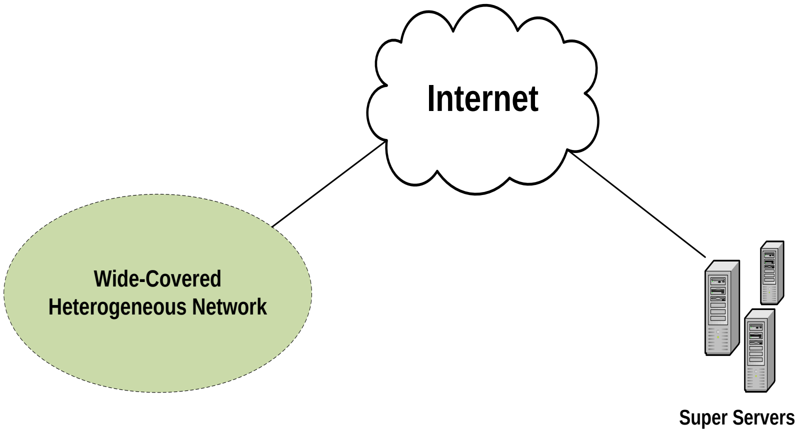


Figure 7.2: A wide-covered heterogeneous network

7.3 BD-MANoN Certificate Management Framework

This section describes the certificate management system of BD-MANoN. It shows how public/private keys and digital certificates are created, and presents the syntax code of the BD-MANoN algorithm. It illustrates the process of certificate revocation. It also shows how the new detection algorithm operates in our MANoN system.

7.3.1 Creation of Public/ Private Keys and Digital Certificate

Like ACM-MANoN, our BD-MANoN algorithm requires a key management service. We have adopted PKI because of its superiority in distributed keys, and its having achieved integrity and non-repudiation. In PKI, each node has its own Public/ Private key pairs. Public keys can be distributed to other nodes, while private keys must be kept confidential to individual nodes.

As already mentioned, each node has its own Public/ Private keys, and each node will receive its own Authentication and Authorisation certificates from its own PKI (MANET). The Authentication certificate will be used as an Identity (Passport), and the Authorisation certificate will be used as a security clearance. Each MANoN's node will hold its certificate in a Local Data Base (LDB). The main structure of BD-MANoN digital certificates is shown in Figure 7.3.

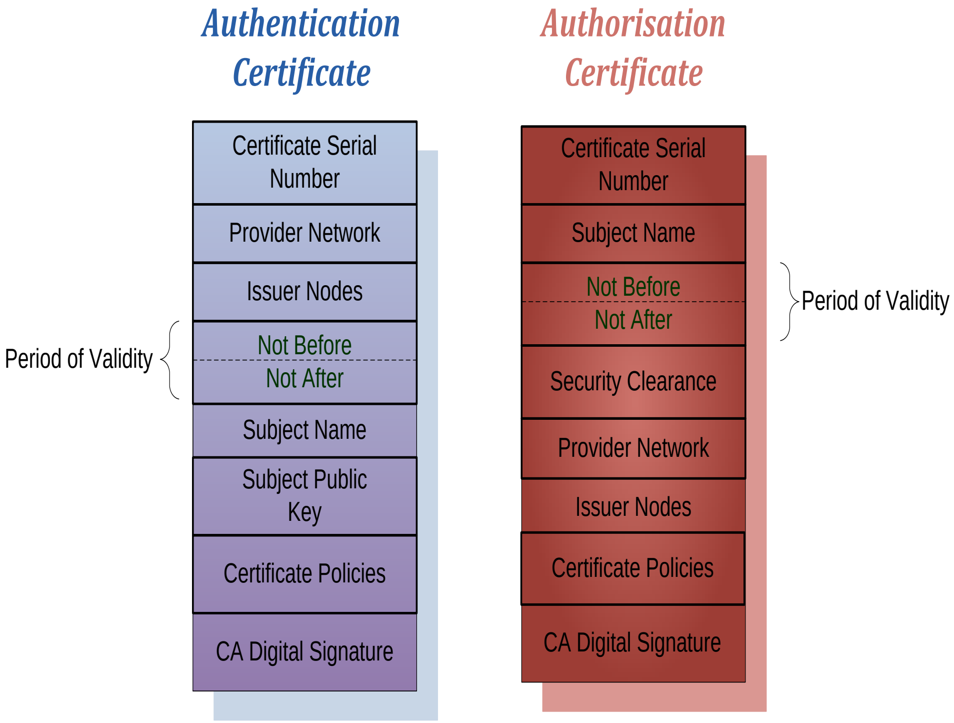


Figure 7.3: The Structure of BD-MANoN Digital Certificates

The certificates contain:

- ***Serial number:*** A unique integer value within the issuing PKI or CA (servers and combiners) that is unambiguously associated with the certificate.
- ***Provider Network:*** Name of the network that issued the certificate.
- ***Issuer Nodes:*** PKI or CA names that created and signed the certificate.

- ***Period of Validity:*** Consist of two dates: the first and last on which the certificate is valid.
- ***Subject Name:*** Holder of the certificates.
- ***Subject's Public-key:*** The public key of the user.
- ***Security Clearance:*** Level of the authorisation certificate which allow the subject to perform in any network with the same priority level (i.e. nodes in a specific network).
- ***Certificate Policies:*** Certificates may be used in environments where multiple policies apply. Therefore, this section will carry a list of policies that the certificate recognises as supporting, together with optional qualifier information.
- ***CA Digital Signature:*** Digital signature having been signed by either the PKI or the CAs.

7.3.2 Implementation of Behaviour Detection

As mentioned above, all nodes receive their keys and certificates (Authentication, Authorisation) from their PKI. Moreover, each MANoN service has its own Public/ Private keys, and all BBN (Servers CA_{Se}, Combiners CA_{C}) will receive a share of the private key (sign certificates and perform threshold cryptography) and the public key in order for CA_{C} to validate other MANoN certificates.

Hence, based on our assumption that an undefined node (*node x*) is trying to engage into our MANoN system, a new authorisation certificate (with less security clearance) will be required which will be produced from our BBN (divided into two types: Local BBN and Global BBN). Since *node x* is undefined in our system, our CAs will not be able to validate its certificates, as the network public key of network x is unavailable; therefore, our BBN will carry out the duty of observing this node.

Therefore, when *node x* from network (1) (Network (1) is undefined in our MANoN) tries to engage and communicate with *node y* from network (2) (Network (2) defined into our MANoN), first of all, *node x* will broadcast his request for an authorisation certificate (to perform in MANoN) attached with his own authorisation and authentication certificates which he had received from his original network. In the second place, after *node x* received its authorisation certificate (provisional), our LBBN and GBBN will carry out the responsibility of observing it. This security clearance may evolve or be revoked, based on *node x* activity in our MANoN system.

As we are dealing with an infrastructure-less MANoN, *node x* will be observed based on his Routing Information Table (RIT); this RIT will show a history of all activities being performed by *node x*. Before defining the observation process, we need to show the architecture components. Figure 7.4 will illustrate the behaviour detection architecture.

The components of our behaviour detection architecture are:

- **General Node (GN):** Regular ground nodes, for example typically soldiers equipped with communication and computation limited devices (Level 1). Its duty is to collect data and transfer them to BBN

- **Local Back-Bone Node (LBBN):** They are usually special units located within the same MANET, for example tanks and personnel carriers which have more extensive facilities than regular ground nodes. LBBN can establish direct wireless links for communication amongst themselves (Level 2). Its responsibility is to collect data and observe nodes entering the MANoN system

- **Global Back-Bone Node (GBBN):** They are usually special units from external networks, for example tanks and personnel carriers which have more extensive facilities than regular ground nodes. GBBN can establish direct wireless links for communication amongst themselves (Level 2). Its duty is to collect data and observe nodes entering the MANoN system

- **Data Collector (DC):** The main buffer of collected data, located in both GN and BBN, enables the behaviour analyser to analyse all available data the system had collected. The data collector will be separated from other components to permit the data collector to operate simultaneously by collecting data from the different resources, and at the same time enables the behaviour analyser to process the transferred information [87]

- **Behavioural Analyser:** The behaviour of the observed node will be abstracted (abstraction are shown below), so it will check whether the behaviour of the nodes is malicious (anomaly, misuse) or normal. The behaviour analyser comprises ***Policy Decider*** and ***Enforcer***. The **Policy Decider** contains a set of policies, which are a set of rules that can dynamically change over time and by events (those policies contain the nature of acts showing the type of behaviour as normal or malicious). The **Enforcer** is a dynamic mechanism that enforces those policies. Checking whether the behaviour of nodes is legitimate is achieved by enabling the enforcer to compare our set of policies with the actual behaviour to decide the nature of the behaviour (shown in detail in section 7.3.2.2)

- **Behaviour Capture:** The behaviour capture stores the history of behaviours that nodes might have (normal, anomaly or malicious) during specific period of time; this capture is always updated depending on the observed node actions, despite the fact that saving all behaviours is impossible; nevertheless, a reasonable number of behaviours must be stored

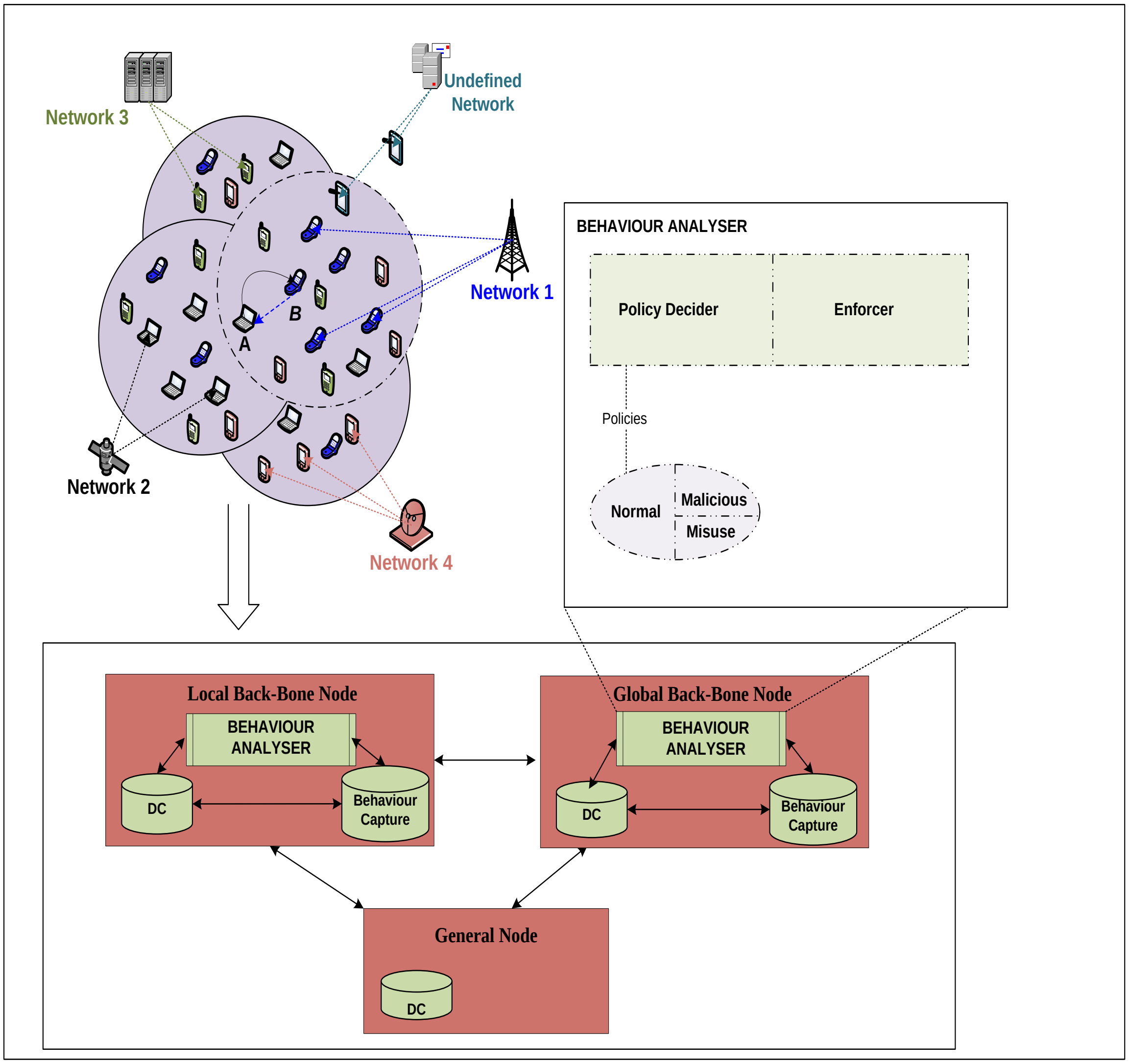


Figure 7.4: Behavioural Detection Architecture

7.3.2.1 Syntax Expressions

Before demonstrating categories of the behavioural detection architecture and implementation of the behavioural analyser, we need to explain our syntax and the variables of our behavioural detection algorithm using Interval Temporal Logic (ITL [67]:

A short introduction is given on ITL to present our policies in a well suited formal description to express behaviour of our BD-MANoN and additionally constrains on the behaviour of our enforcement mechanism that represent policies.

- P : is a property; a property P is a formula written in underlying logic (e.g. using ITL)
- h_i : is the behaviours $i,\ i \geq 1$;
- σ_i : is a states $i,\ \ i \geq 1$;
- T : is a trace which is a portion of h_i;
- Var : is a set of interesting variables;
- Val : is a set of semantic values.

The key concept of ITL is State σ_i. State is considered to be a (in)finite sequence of states, where State σ_i is a function from the set of variables to the set of values.

$$\sigma_i : Var \rightarrow Val$$

Behaviour h_i is a sequence of States σ_i,

$$h_1 \triangleq \ \sigma_1\, \sigma_2\, \sigma_3 \ldots$$

Trace T is a portion of Behaviours h_i

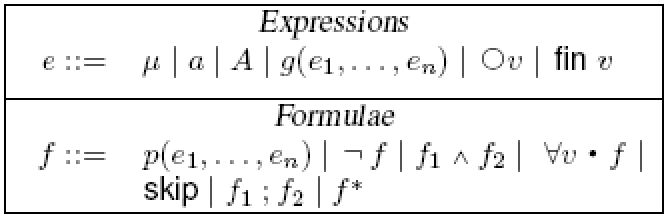
We are seeking to prove that a given observation (Trace) will satisfy a Property.

$$T\ sat\ P \ldots (1)$$

To show the satisfaction, we consider (1) as a semantic level.

$\llbracket P \rrbracket \triangleq$ Set of all possible behaviours, each satisfying the Property P

The syntax of ITL is defined in **Table 7.1** where μ is an integer value, α is a static variable (does not change within an interval an interval), A is a state variable (can change within an interval), v a static, g is a function symbol and ρ is a predicate symbol.



	Expressions
$e ::=$	$\mu \mid a \mid A \mid g(e_1, \ldots, e_n) \mid \bigcirc v \mid \mathsf{fin}\ v$
	Formulae
$f ::=$	$p(e_1, \ldots, e_n) \mid \neg f \mid f_1 \wedge f_2 \mid \forall v \bullet f \mid$ $\mathsf{skip} \mid f_1 \mathbin{;} f_2 \mid f^*$

Table 7.1: Syntax of ITL

The informal semantics of the most interesting constructs are as follows:

- skip: unit interval (length 1, i.e., an interval of two states).

- f_1 ; f_2: holds if the interval can be decomposed ("chopped") into a prefix and suffix interval, such that f_1 holds over the prefix and f_2 over the suffix, or if the interval is infinite and f_1 holds for that interval. Note the last state of the interval of the interval over which f_2 holds.

- f^*: holds if the interval is decomposable into a finite number of intervals such that for each of them. f holds, infinite number of finite intervals for which f holds

- Ov: value of v in the next state when evaluated on an interval of length at least one, otherwise an arbitrary value.

- Fin v: value of v in the final state when evaluated on a finite interval, otherwise an arbitrary value.

Following are some samples of formulas with their informal meaning.

- $I = 1$ holds for an interval if *I*'s value in the initial state is equal to 1.

- skip; $I = 5$ holds for an interval if *I*'s value in the interval's second state is equal to 5.

- $I = 1$; $I = 3$ holds for an interval if *I*'s value in the initial state is equal to 1 and the value of *I* is equal to 3 in some other state (not necessary the second) of the interval.

- $\neg$(true; $I = 0$) holds for an interval if *I*'s value is never equal to 0 within the interval.

Obviously common temporal modulates such as $\Box$ (always) and $\Diamond$ (sometimes) can be expressed. Following are few ITL examples:

The statement "*I is always greater then 2 and some times less then 5*" can be expressed by the formula

$$\Box\ (I > 2) \wedge \Diamond\ (I < 5)$$

Meanwhile, the formula

$$\Diamond\ [(I = 1) \wedge \Diamond\ (I = 2)]$$

Describes an interval of time in which the variable *I* at some time equals 1 and at some later time equals 2. Properties of time can also be expressed. For instance, if *I* always equals 1 and *J* sometimes equals 3 then we can infer that the sum *I*+*J* sometimes equals 4:

$$[\Box\ (I = 1) \wedge \Diamond\ (J = 3)] \supset \Diamond\ (I + J = 4)$$

These examples express only a indistinct idea of the utility and convenience of temporal logic. As will be shown, temporal logic offers a natural means for recounting such dynamic notations as stability, termination and interval length.

7.3.2.2 Behavioural Analyser

As depicted in Figure 7.4, each BBN will embrace a behaviour analyser. The structure of the behaviour analyser consists of the policy decider and the enforcer. The policy decider uses a set of policies (properties) to decide whether behaviour is malicious or not. At the beginning, we define all policies as normal policies (indicating good behaviours), and during the running of the system, some of those policies will be dynamically changed into malicious policies (indicating anomaly, misuse behaviours) based on specific actions and events the system might go through. Moreover, normal policies will not stay mandatory good, as those policies are dynamic, and different situations might change them into malicious policies. Meanwhile, the enforcer is a mechanism that enforces those policies. The mechanism of enforcing those policies will dynamically change based on specific actions and events. (For example. when security alerts in airports are elevated in any country, different procedures will be put in place to handle the security situation). Evaluation details will be shown in chapter 8 (case studies).

After defining the structure of our behaviour analyser, we will use the policy categories as a comparison model to check new node activity, and whether those activities are normal or not. Therefore, the question now is: how does our behaviour detection operate?

When *node x* tries to operate in our system, the GN and BBN will audit the data from the RIT of *node x*; basically these audit data will create the state of *node x.* In other words, our audit data is originally the function from the set of variables to the set of values. As a result, a new state of *node x* will be created whenever there are new data in the RIT, example of the RIT is shown in **Table 7.2**.

RREP	T	F
RREQ	F	T
DROP	F	T

Table 7.2: Route Information Table for Node x

Table 7.2, shows that each state is created from the new entry in the RIT for instance: $[RREP \wedge \circ\ RREQ \wedge \circ\ DROP]$ from the equation each action is a state which is a function from a set of variables to the set of values. Moreover, Figure 7.5 shows how new states are created by RITs data.

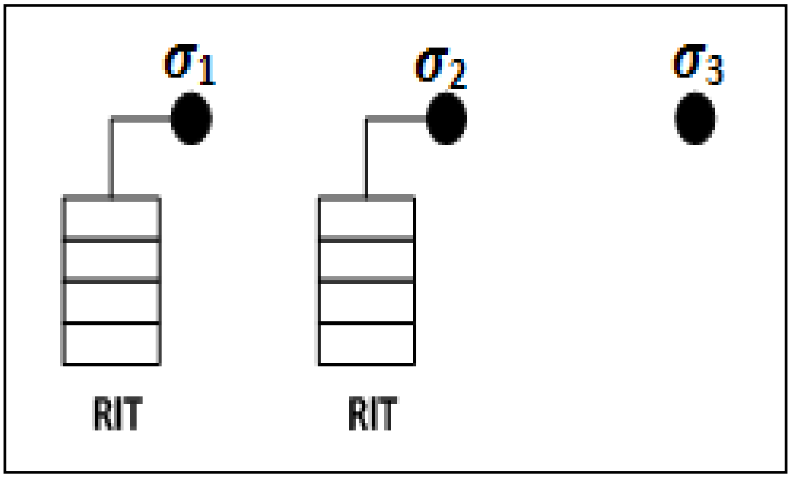


Figure 7.5: Creation of States

The sequence of these states will create the behaviour, and since there is an infinite number of behaviours it is impossible to observe all types of behaviour. Therefore, our observers try to make an observation on *node x* activity; they will slice a trace of *node x* behaviour and try to satisfy it with our properties to find if *node x* activity is legitimate or not and in which category it belongs.

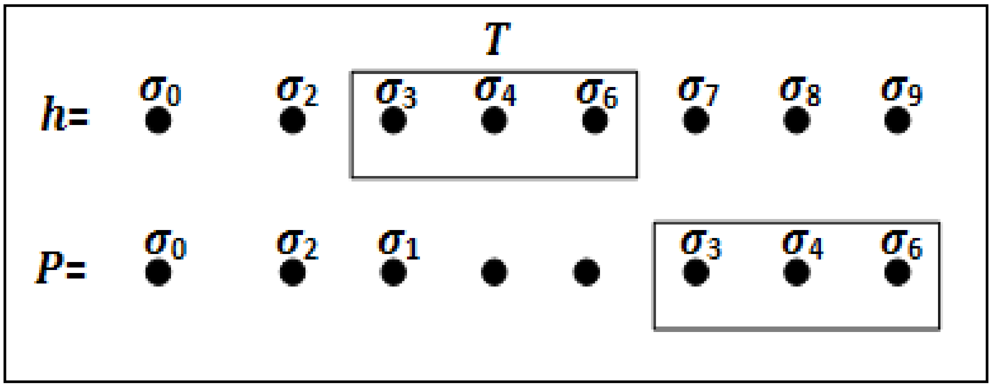


Figure 7.6: Trace satisfies a Property

As can be seen in Figure 7.6, *h* represent the behaviour of *node x*, while *T* is a slice of *node x* observed behaviour, so that a comparison with our *P* can be made to find whether or not this behaviour is found to be identical to our policy category; if not our BBN will try to analyse the manoeuvre of *node x* behaviour in a specific period of time by collecting more data. Eventually, it shows whether the behaviour is going towards a diversion or normal act.

For example, if *node x* was discovered attempting to enter a specific area, he is not allowed to enter or to endeavour to access a specific log file, when it did not have the authorisation to do so; this behaviour will be considered as malicious or misuse.

After a specific period of time and based upon the BBN observation, a decision will be taken to decide whether to upgrade or revoke nodes certificates. This mechanism is shown in our publication [4].

7.4 Coping with Misbehaviour Users

In the BD-MANoN algorithm, it is easier for malicious nodes to make other nodes accept false certificates. This is because some certificates are issued by undefined CAs, networks or even certificates signed by the nodes themselves. In these cases, our BBN will carry out the observation task to distinguish the malicious from the normal nodes; some malicious node examples which have been recognised by our BD algorithm are given here:

- *Forging Sequence Number (SN)*

  In AODV, Sequence Number (SN) plays the task of guarantying loop-free routes and indicates the freshness of the routing information. SN increases under two conditions: when destination node replies with RREP and when source node request with RREQ; as a result, the SN updates only by the source and destination [93].

  Forging sequence number is a single attack type that can be launched from an insider node on an AODV routing protocol. As mentioned the SN refers to the freshness of route of the associated node. Whenever the SN is forged by a high number from an attacker the route will be changed towards the higher SN route.

  For example, when employing the AODV routing protocol in our MANoN scenario (see Figure 7.7), if source A tried to connect destination D, the normal route will be {A,B,C,D} but if M sends RREP m2 to B with SN.Dst equal to 100 (>50 normal replay), it will take precedence over c2; with the same method to B, M can control the route between A and D (creating man in the middle attack).

Our policy states that:

Given node I,
I_{Src} denotes current SN.Src
I_{Dst} denotes current SN.Dst
Max_{Src} denotes maximum SN.Src
Max_{Dst} denotes maximum SN.Dst

$$\Box\, [\neg ((I_{Src} > Max_{Src}) \vee (I_{Det} > Max_{Dst}))]$$

If SN.Dst and SN.Src of any nodes' packet is much greater than it should be, this act will be considered as malicious (an attempt to create man-in-the-middle attack)

Given node I,

$$\neg\, [\Box\, ((I_{IP} \neq Src_{IP}) \vee (I_{IP} \neq Dst_{IP}))]$$

If the packets are sent from nodes' IP address that is not equal to the original source IP address or original destination IP address (shown in the routing forwarding table), it will be considered as a malicious act

This attack can be detected and dealt with by our BBN. According to our BBN, the forwarding table in BBN SN.Dst=50. Based on our policies, if our BBN nodes detect any packets having SN that is much larger than it should be (100), or that packet has not been sent by the owner of SN (IP address is not equal to the source), then the BBN will treat it as an attack.

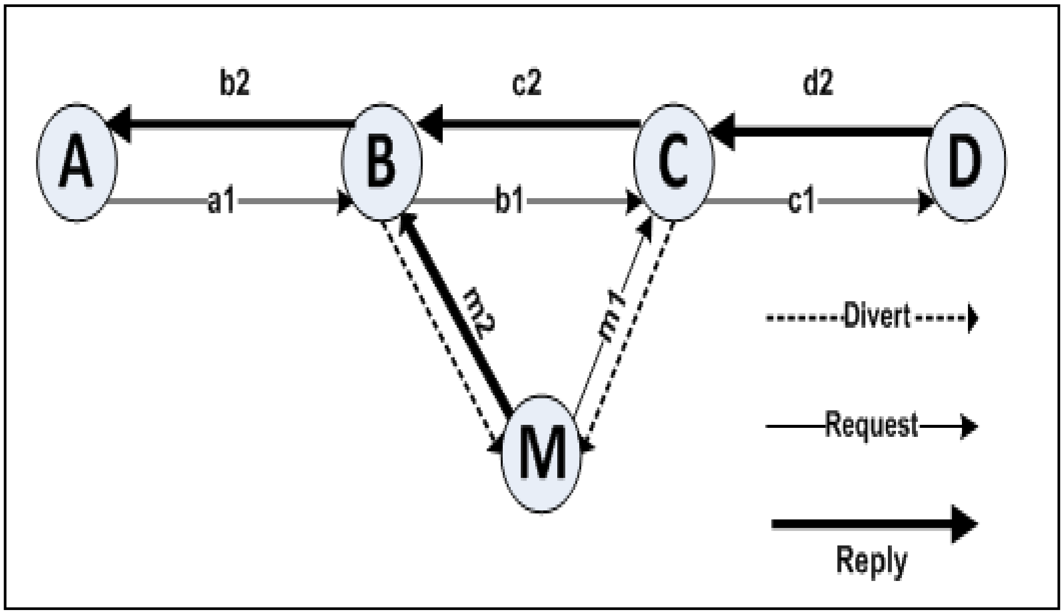


Figure 7.7: Man in the Middle Attack

- *Wormhole Attack (Tunnelling)*

This is a cooperating attack done by two malicious nodes; an attacker receives packets at one location in the network and tunnels them to another location in the network, where packets are re-sent into the network (creating a traffic route through them) [48].

As shown in Figure 7.8, if A wanted to connect E, the shortest path will be {A,B,C,D,E}; instead, X will pretend to have a direct connection to Y, creating a false short path {A,X,Y,E} which will enable A to choose the wrong path which is actually {A,X,B,C,D,Y,E}, preventing A from to choosing the really short path {A,B,C,D,E}.Even cryptography solutions, such as ARAN [97] cannot hinder this kind of attacks. Let ℓ be a Boolean function which is defined as:

$$\ell : \mathcal{N} \times \mathcal{N} \longrightarrow Bool$$

For any two nodes, n_1, n_2 if ℓ (n_1, n_2) = true, then a link between n_1, n_2 exist, otherwise the nodes are not connected.

ℓ denotes whether there is direct link between $n_1$and n_2 and its defined as follows:

$\ell\colon \mathcal{N} \times \mathcal{N} \longrightarrow Bool$

$\ell\ (n_1, n_2)$= true *iff* there exist a direct link between $n_1\ and\ n_2$.

Our policy states that:

$$\forall\, n_1, n_2\ \in N.\, \Box\, \ell\ (n_1, n_2)$$

Based on Figure 7.8, by checking the IP.Header of any node (X) gets a RREP which is essentially not from the exact node (Y) that X is claiming; therefore, X will be considered as malicious and the connection between X and Y is fake.

Based on our behaviour detection, the solution is simple: whenever our BBN checks the RIT of node Y, it will find that the RREP is not from X; therefore, our detection algorithm will detect that the route between X and Y is actually false.

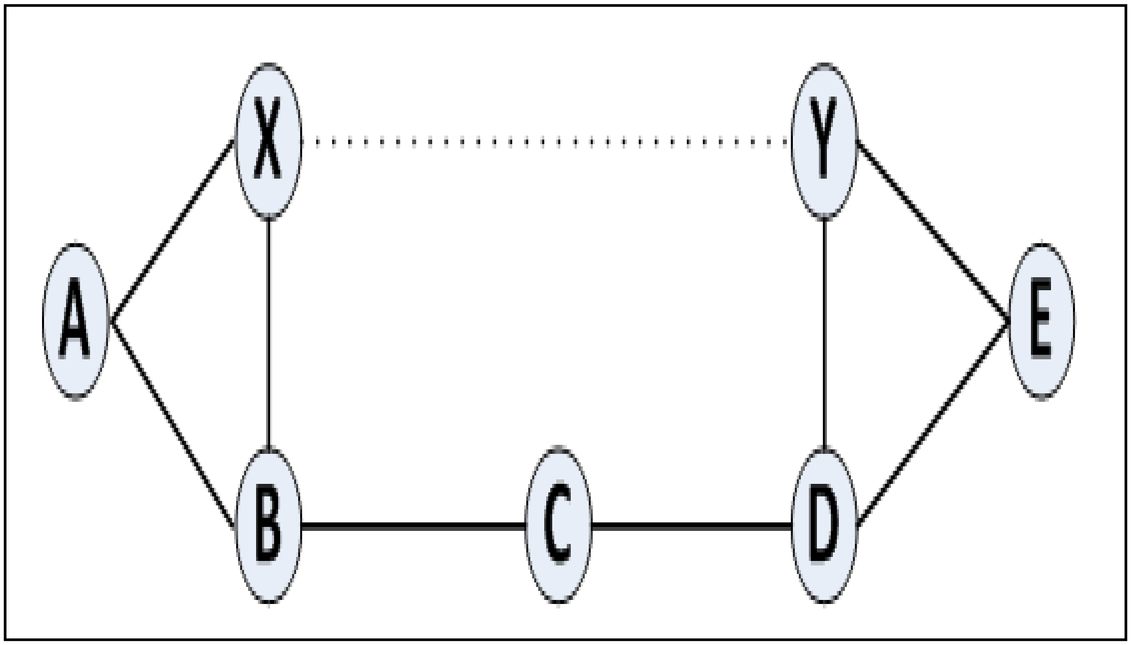


Figure 7.8: Tunnelling Attack

7.5 Summary

As mentioned before, providing security management in our MANoN is our main goal, which will be achieved by providing the essential component prevention and detection. In chapter 6, prevention is presented in our ACM-MANoN mechanism, and has been evaluated using the NS-2 simulation tools. However, providing detection is much harder to deliver, as ad hoc networks are decentralised and infrastructureless nevertheless, in this chapter we have presented a novel behaviour detection algorithm, BD-MANoN, based on threshold digital certificates. This detection algorithm is abstracted from variables of the route information tables (RIT) of each node, in which the Back Bone Nodes (BBN) can decide whether nodes in any part of the MANoNs are malicious or normal. This decision is made based on a set of dynamic policies used to compare old with new behaviours in order to make such decisions. Actual examples are shown, to prove that the policies for “forging sequence number” and “wormhole attack” are indeed sufficient to detect and prevent such attacks.

Moreover, this algorithm will be evaluated using specific case studies such as military environments. These will illustrate the enforcement of dynamically changing security policies.

Chapter 8

Evaluation & Case Studies

Objectives

- Illustrate a military case study
- Illustrate our ACM-MANoN
- Illustrate our BD-MANoN with different scenarios

8.1 Introduction

Mobile ad hoc network of networks are considered to be the future of wireless networks owing to their specific characteristics (practical, simple, self-organization, self-configuration, ease of use and inexpensive when operating in a licence-free frequency band).

There are many applications to ad hoc networks, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, having highly dynamic mobility such as:

- In education, ad hoc networks may be deployed for student laptops interacting with the lecturers during classes
- Health care and telecare systems
- Inter-Vehicle Communications, ad hoc networks for vehicles, for example, sending instant traffic reports and other information between drivers
- Electronic email and file transfer
- Web services that can be used by ad hoc network users in case a node in the network serves as a gateway to the outside world

- A wide range of military applications, such as a battlefield in unknown territory where an infrastructure network is not available or impossible to maintain
- Collaborative work for business environments
- Emergency search-and-rescue operations, in disaster areas where it is almost impossible to implement an infrastructure network
- Personal Area Networking (PAN) and Bluetooth
- Electronic payments from anywhere (i.e. taxi)
- Home Wireless Network and smart homes
- Office Wireless Network

In this chapter, we evaluate our security management system, with concentration on *Access Control Prevention* and *Behaviour Detection* techniques. A military case study with two scenarios will be introduced: the first scenario study will highlight our security management system, with concentration on our *Access Control prevention* technique (explained in chapter 6) for predefined armies in an unknown and unstable MANoN military environment system; this scenario will combine authentication, authorisation, confidentiality and integrity to provide a privacy protection for elements and tactics.

The second scenario study illustrates a security management system in an unstable and unknown military environment, showing *Behaviour Detection* techniques combined with policies, and carried out to provide a secure military system against unknown elements.

8.2 Case Study 1: Military Environment

This military case study shows a battlefield in unknown territory, where infrastructure deployment is hard to achieve or maintain; therefore, MANoN will be the perfect solution to such a scenario. As known, the military domain is a very challenging environment described by ambiguity and the need to be able to deal with significant and disruptive dynamic changes. The military system goal is mainly concerned with the ability to satisfy a secure environment for its components, because opponents (enemies) are always trying their best to break down or destroy our activities. Therefore, our security management concentrates on prevention and detection mechanisms.

8.2.1 Components Definition for Military Environment

In the military environment, a critical system and the specification of the security requirements for its components are essential. *Authentication* and *Authorisation* are one among most important requirements to be fulfilled, but before defining and analysing these requirements, we need to define our military system and its elements.

We will be dealing with a military alliance consisting of different armies (e.g. NATO [82]); each army will be defined as a MANET, whereas the whole alliance is defined as MANoN. Each one of those armies includes different elements, starting from a soldier to the commander-in-chief (officer). Usually in the military, the officers will have a specific hierarchy, in which each officer will have the authority to give orders or to communicate with different elements based on his/her military ranking in the system.

- Each army will be classified as MANET
- Merger of MANETs creates the whole military alliance which is a MANoN
- Officers are based on hierarchical ranking
- Soldiers in our MANoN will be defined as normal ad hoc nodes
- Specific high ranked officers (e.g. Majors, Brigadiers and Generals) are defined as Back Bone Nodes (CA)
- A set of policies will be defined in each MANET (army)

8.2.2 Securing the Military Environment

Our military alliance will be a merger of different MANETs creating the MANoN. MANoN are dramatically shown in Figure 8.1. The first step in providing a secure military system is providing authentication between the MANoN components; this authentication process is granted by distributing the authentication certificates, which is initially granted from the MANET base station. This authentication certificate acts as an identity for each element in the MANoN military environment.

As with the authentication certificates, the same elements will initially receive their authorisation certificates from their MANET base station; each certificate holds a specific security clearance to enable specific nodes to carry out leading and agile operations, and to give orders to different soldiers and officers.

To cover our security management and to highlight the security mechanisms defined in previous chapters, we will show different scenarios for the military environment.

Scenario One

This scenario configures a military alliance with three armies (US, Canadian and British); each one of those armies will have a specific priority upon the other. For instance, the US will be categorised as priority one (Highest), while Canada will be categorised as priority three.

This categorisation will be used to classify our authorisation certificates in each MANET. Before defining the ACM-MANoN to provide authorisation and authentication to other nodes, a few points must be clarified in our scenario:

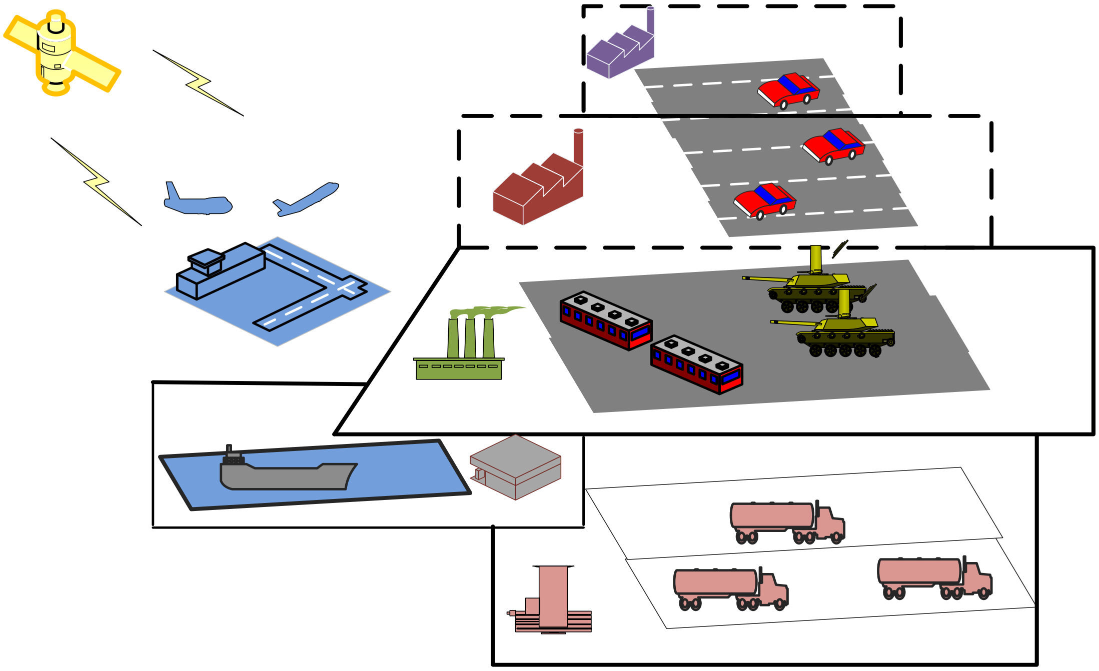


Figure 8.1: MANoN community

- Armies can join and disconnect without affecting the MANoN system
- The public keys of the digital certificates are known between all elements in the whole MANoN system
- All nodes (soldiers and officers) have received their authentication and authorisation certificates from their own MANET (each army has its own certificate)
- Each MANET has a set of policies

To provide security management to this scenario, the first step is to show our administration; as previously mentioned, the BBN (high ranked officers) will carry out the administration duty. Their duty is to guarantee that elements from different armies can communicate and engage with different elements in the MANoN system.

The second step is to provide the most essential components' prevention and detection, which are needed in any community. Such prevention and detection are needed for the authentication and authorisation of the MANoN elements. For instance, a lieutenant from the US army is trying to lead a Canadian platoon; this Lieutenant will be authenticated (verified) from the BBN of the Canadian army by his authentication certificate. Meanwhile, an authorisation certificate will be granted with a brigadier ranking, based on the policies (the priority of the Canadian army is less then that of US army) of the Canadian army to lead the platoon.

The third step, is the containment and recovery component; usually, whenever a problem has occurred during any military operation, specific rules and procedures will take place; for example, if members of the Canadian platoon have been captured by the enemy, the enemy will try its best to extract the private key in order to gain access to all secret information, and to forge new certificates in order to break the system down. In this situation, the BBN of the Canadian army will try to re-generate new shares of the private key, to make sure that the private key is kept safe during military operations.

Moreover, a periodic update of information via links through heterogeneous cards available with BBN (e.g. satellites and cellular) will be used to receive orders from the main station of the network to which the BBN belongs.

To elaborate more on our security management system, and to show the authentication and authorisation components provided between the military elements in the ACM-MANoN, specification formalism will be introduced:

$X_{i\,j}$: soldiers i from the army j, $i \geq 1$; j countries from the NATO;

$Y_{i\,j}$: officers i from the army j, $i \geq 1$; j countries from the NATO;

Authentication and Authorisation between elements from the same army (US) in the MANoN military system

Authentication ($X_{1\ US}$, $X_{2\ US}$) between US soldiers in the same army is achieved based on the *X* authentication certificate, where *X* is received from the US base station. The certificate will be verified using the US public key. Similar to the authentication certificates, the authorisation certificate will hold a specific security clearance, and will be verified using the US public key.

Authentication ($Y_{1\ US}$, $Y_{2\ US}$) between US officers in the same army is achieved based on the *Y* authentication certificate, where *Y* is received from the US base station. The certificate will be verified using the US public key. Similar to the authentication certificates, the authorisation certificate will hold a specific security clearance, and will be verified using the US public key.

Authentication ($Y_{1\ US}$, $X_{2\ US}$) between US officers and soldiers from the same army is achieved based on *Y* and *X* authentication certificates, where *Y* and *X* are received from the US base station. The certificates will be verified using the US public key. Similar to the authentication certificates, the authorisation certificate will hold a specific security clearance, and will be verified using the US public key.

$X_{i\,j}$: soldiers i from the army j, $i \geq 1$; j countries from the NATO;

$Y_{i\,j}$: officers i from the army j, $i \geq 1$; j countries from the NATO;

Authentication between elements from different armies (US, Canada) in the MANoN military system

Concerning a*uthentication* ($X_{1\ US}$, $X_{1\ Canada}$), if a soldier from the US army wanted to authenticate a Canadian soldier, this will be verified using the Canadian authentication certificate. The certificate will be verified using the Canadian public key (public keys are distributed between the predefined armies in the whole military). In addition, if a soldier from the US tries to communicate with a Canadian soldier, then the US soldier will need an authorisation certificate from the Canadian army; this is granted by the BBN of the Canadian army, allowing communication with the Canadian soldier, based on the original authorisation certificate the US officer holds with respect to the ranking policy (security clearance) the certificate holds.

Concerning *authentication* ($Y_{1\ US}$, $Y_{1\ Canada}$), if an officer from the US army want to authenticate a Canadian officer, this will be verified using the Canadian authentication certificate. The certificate will be verified using the Canadian public key. Meanwhile, if an officer from the US army tries to help or give an order to a Canadian officer, an authorisation Canadian certificate is required, which can be granted from the BBN of the Canadian army, based on the original authorisation certificate the US officer holds with respect to the ranking policy (security clearance) the certificate holds.

With reference *to authentication* ($Y_{1\ US}$, $X_{1\ Canada}$), if an officer from the US army wants to authenticate a Canadian soldier, this will be verified using the Canadian authentication certificate. The certificate will be verified using the Canadian public key. Meanwhile, if an officer from the US army tries to lead or give an order to a Canadian platoon, an authorisation Canadian certificate is required; this can be granted by the BBN of the Canadian army, based on the original authorisation certificate the US officer holds with respect to the ranking policy (security clearance) the certificate holds.

Scenario two

As with the first scenario, scenario two configures a military alliance consisting of three armies (US, Canadian and British), and each one of those armies will have a specific priority upon the other. For instance, the British army will be categorised as priority one (highest), while the, Canadian army will be categorised as priority three. In addition, new elements will be defined in this scenario (Japanese army, Red Cross and Red Crescent).

This categorisation will be used to classify our authorisation certificates in each MANET. Before defining the BD-MANoN to provide authorisation and authentication to other nodes, some points must be clarified in our scenario:

- Armies can join and disconnect without affecting the MANoN system
- The public keys of the digital certificates are known between some (US, British and Canadian) elements in the whole MANoN system and unknown to others (Red Cross, Red Crescent and Japanese army)
- All nodes (soldiers and officers) have received their authentication and authorisation certificates from their own MANET (each army has its own certificate)
- Nodes that are undefined and trying to operate in different networks will receive a provisional authorisation certificate
- Each MANET has a set of policies

To elaborate on our security management system and to show the authentication and authorisation components provided between the military elements profundity in the BD-MANoN, the following example is introduced:

If during war the British army needs reinforcements from Japan (example) and Japan is a non-NATO country, in order for the Japanese army to communicate with British forces and to engage into the battlefield, Japanese soldiers and officers will need to obtain a provisional certificate from the British BBN to perform in such situations.

As Japanese forces are non-trusted, our BBN will monitor and observe their actions based on their RIT in order to check whether or not Japanese elements are acting in a normal or malicious manner. This checking is accomplished by comparing a trace of behaviours with the set of policies the British army has defined.

Usually, showing all situations of comparing the trace of behaviours with the set of policies in our scenario is impossible; therefore, we provide different examples showing normal and malicious actions.

In the first example, set during the war, if an order from a British officer has been given to Japanese troops and the soldiers did not obey these orders to follow an order from a higher ranked officer (conflict of orders), then our BBN will try to observe these acts and decide whether or not the act is normal; this is determined by a check against British policies. It is assumed that this policy will declare:

- If an order from a higher ranked officer has been given, this order will be obeyed from all troops unless a conflict of orders with a higher ranked officer has occurred

Therefore, based on this policy, the behaviour of the Japanese nodes will be considered to be normal when checked against this rule.

In the second example, set during the war, an officer from the Japanese army holds a low ranked authorisation certificate and tries to request a specific tactic from other officers in the British army (assuming our policy decline this request). Therefore, our BBN will try to observe this act and decide whether or not the act is normal; this is decided by checking the British policies. It is assumed the following exists:

- If elements are trying to access unauthorised area or request unauthorised tactics consequently, such elements will considered to be malicious

For that reason, the behaviour of the Japanese officers will considered to be malicious, and appropriate action will be decided upon towards the malicious elements.

After showing normal and malicious behaviours being compared with pre-existing policies, the question will be: what if a specific behaviour or action was not found in our policies? For this situation, the trace of the behaviour can not be compared with any set of policies in the system, as that trace does not satisfy any of the policies. Therefore, our BBN will analyse the RIT comparing elements actions with similar policies to find whether the act is going towards a deviation or a normal act.

For example, during the war, if elements switch off their devices - either to constrain power or for any other reason - the BBN will try to analyse the data and check if that switching is happening consistently. If so, this act will count as a deviation towards malicious behaviour. On the other hand, if it happens only once, then the BBN will consider it as normal behaviour.

In the final example, if in the middle of a war, a truce (ceasefire) has been announced, then usually the Red Cross or Red Crescent will try to secure and rescue injured parties and provide health care to civilians. In this situation, the Red Cross elements will hold a provisional authorisation certificate, which will be granted by the BBN from the army with which they are operating.

During the operation of the Red Cross, observations will take place upon those elements to make sure that the operation is as it is supposed to be. In other words, they are not acting maliciously to gain secret information for the enemy. During these observations, a trace will be taken from the RIT of the Red Cross and a comparison against the army policies will be performed.

An example, of such policies is the following:

- During normal situations, officers and soldiers are eligible to communicate with outsider nodes or networks, but during war, every communication to an outsider network or node is considered to be a malicious act

Based on this policy, ‘ceasefire’ is not defined in our policies, so whenever members from the Red Cross try to communicate to an outsider node, the act will be considered as normal (as we are in ceasefire) but based on the situation (Red Cross members are not fully trusted) in which our dynamic BBN’s enforcer will monitor actions extracted from the RIT of the Red Cross members. Therefore, the enforcer in the BBN will make ensure that such behaviour is considered as normal or malicious, based on the evidence the BBN has collected.

8.3 Summary

In this chapter, different case studies have been provided with specific concentration on a military case study in unknown and unsecure territory. This case study presents two scenarios.

Scenario one defines three NATO countries (pre-connected) in a battlefield; each country holds a specific security clearance (ranking) over the other. This scenario shows the implementation and evaluation of our Access Control Mechanism (ACM-MANoN) providing authentication and authorisation between members of the same network and between other members of the MANoN.

Meanwhile, scenario two defines three NATO countries with new elements (non-defined); this scenario shows the implementation and evaluation of our Behaviour Detection mechanism (BD-MANoN), showing the detection technique between the NATO countries and the undefined elements, presenting different situations any military system might experience. Each situation gives a comparison with our policies to establish whether or not this situation satisfies our set of policies in order to detect malicious acts of the undefined elements in the MANoN military system.

Chapter 9

Conclusion and Future Work

This chapter summarises our findings, highlights the contributions and suggests directions for future work.

9.1 Summary

The growing interest in MANoN techniques has resulted in many communication and security protocol proposals. Security issues in ad hoc networks are currently attracting increasing attention.

MANoNs are particularly vulnerable to attacks. This is because of their features of open medium, dynamic changing topology, lack of centralised monitoring and management point and the lack of a clear line of defence. A full description regarding MANoN general information was introduced in chapter 2; it contained a discussion of the history and background, characteristics, challenges and network security concentrating on security requirements, attacks and full analysis of cryptography background regarding symmetric, asymmetric, digital certificates, PKI and trust.

Security Management is a central aspect of security in MANoN. Solutions to the problem of public key management, intrusion detection and prevention techniques for security management in MANoN were presented in Chapter 3. Some of these solutions try to adapt the hierarchical trust model in order to provide secure, available key management services, such as the Z-H scheme and MOCA. Most of these solutions define a virtual CA using threshold cryptography. This CA comprises multiple mobile nodes that collectively provide certification services. These solutions are quite elegant and potentially offer a good measure of security and availability.

Solutions regarding intrusion detection, such as providing a distributed intrusion detection system based on mobile agents technology, are also included. It provides a lightweight and low overhead mechanism to detect anomalous nodes in the system. A different approach is to use local and collaborative decision-making in anomaly detection. In this approach, each ad hoc node participates in detecting locally and independently malicious acts. Each node holds an individual IDS agent that monitors local activities, which enable it to detect local traces and respond to it [70 – 72].

On the other hand, different security management schemes have been proposed; these include a Novel Computational Reputation Model for Wireless and Mobile Ad hoc Networks, which provides a prevention technique based on trust and reputation. This type of security management focuses on prevention technique, as it presents a set of management mechanisms based on trust and reputation to prevent malicious nodes from entering the trusted community. Moreover, depending solely on the trustworthiness and reputation of nodes is not suitable for applications where high degrees of accountability and security are required [5, 29, 112].

In addition, a security management in a hierarchal system is introduced; this combines both threshold cryptography and cluster-head to distribute keys to its nodes, but does not provide any actual type of security management to the ad hoc networks.

Solutions to MANoN's security problems in general and to security management in particular should be built upon a strong foundation. This means constructing a specialised security management for MANoN that helps in modelling it, addressing security challenges, defining security attacks and security requirements, and describing principles and plans to achieve all the objectives of these security requirements and then proposing security mechanisms that enforce the implementation of these objectives. This methodology for securing MANoN was followed in Chapters 4-8.

Chapter 4 defined this security management architecture, based upon the two ITU-T Recommendations, X.800 and X.805 that are used to define security architecture for a MANoN. The security architecture proposed a technology-independent security solution for a MANoN, which provides end-to-end communication that can be implemented using different security mechanisms.

In Chapter 5, we presented a security management technique of two different mechanisms. Each mechanism defines one scenario. Chapter 6 expounded the first algorithm (***ACM-MANoN***), which manages the digital certificates in a fully defined MANoN environment, and then provided an evaluation using the NS-2 simulator. The second algorithm (***BD-MANoN***), which manages the digital certificates in a partially defined MANoN, was presented in Chapter 7 with an evaluation, also using a formal description and attacks case study. A military case study is presented in Chapter 8.

9.2 Contributions

The main contributions of this work to the existing literature on the subject are the definition of the novel the new comprehensive security architecture for MANoN. The security architecture is unique in the respect that no comparable proposal has been made. In addition, a security management system concentrating on two security algorithms has been proposed to manage digital certificates in a MANoN in two different scenarios. The heterogeneous environment assumption and the way it is used in defining these algorithms is of itself a novelty. The contributions are detailed in the following sections.

9.2.1 Security Architecture for MANoN

The definition of the security architecture is based upon the two ITU-T recommendations, X.800 and X.805, which help in locating the global security challenges facing MANoN, realising their solutions, and providing the specification of a comprehensive, end-to-end security solution for MANoN that can be applied to any similar wireless service scenario exploiting such networks in order to predict, detect, and correct security vulnerabilities.

The proposed security architecture identifies seven security requirements including *authentication, authorisation, privacy, data confidentiality, availability, data integrity* and *non-repudiation* that protect against major security threats attempting to attack MANoN. Such attacks are generated accidentally or intentionally, internally or externally and are active or passive. A methodical approach for securing MANoN has been illustrated by taking each proceed between any two of the components as a unique perspective for consideration of the seven security requirements, and presenting eight tables describing the objectives of these requirements for each proceed. In order to implement the objectives of the security requirements defined in these eight tables, a set of security mechanisms is needed.

9.2.3 Security Management and Security Mechanisms for Managing Digital Certificates in MANoN

Security in a MANoN can be achieved in two ways [119]:

- ***Proactive security:*** prevents the MANoN from attacks
- ***Re-active security:*** detects the intruders or malicious users and excludes them from the network

The research regarding proactive security is mainly about attacks prevention; in respect of reactive security, that primarily concerns the architecture in which to observe the network, the useful information to be gathered for intrusion detection, and to react to attacks.

The present thesis is interested in both proactive securities that attempt to prevent an attacker from launching attacks in the first place, typically through different cryptographic techniques. In addition, the reactive approach tries to obtain and detect security terrorisation and react accordingly.

Therefore, a security mechanism for managing the digital certificates in MANoN was proposed. This security mechanism implements the objectives of *authentication, authorisation, availability, data confidentiality, data integrity* and *non-repudiation* of proceeds (1), (2), (7) and (8), defined in the MANoN security architecture.

The security mechanism assumes a heterogonous wireless environment in which MANoN operates in an area covered by other infrastructure-based wireless networks, such as WLANs and cellular systems. This security mechanism proposes two algorithms for two different scenarios.

The first algorithm, called ***ACM-MANoN***, tackles the issue of managing the threshold digital certificates in cases in which all the MANoN nodes are defined to other infrastructure-based wireless ad hoc networks. This algorithm provides a prevention technique against malicious nodes trying to break the system.

The second algorithm, ***BD-MANoN***, assumes as a part of its network model that some MANoN nodes are defined to other wireless ad hoc networks. This algorithm is carried out to distinguish and detect malicious nodes from inside and outside the system. This detection is achieved through behaviour detection.

This combination improves the security level by using threshold cryptography PKI, and simultaneously giving MANoN nodes the opportunity to participate in key management system services.

These two algorithms have been evaluated in two ways, as shown below:

- ***NS-2 based evaluation:*** The performance of the ACM-MANoN algorithm is tested in a real network environment, and their communication cost is measured using the NS-2 simulator, which was suitable for the present purpose. The evaluation metrics used in this study are success ratio, delay, average number of retries and overhead. Moreover, a formal description regarding the ACM-MANoN prevention is provided.

- ***Military Case Study:*** the performance of the BD-MANoN is evaluated using a formal description. In addition, a military case study in an unknown and unprotected environment is provided to show a real example of behaviour detection.

9.2.3.1 ACM-MANoN

ACM-MANoN proposes a security protocol for managing digital certificates in a pre-defined environment. It is based on the hierarchical trust models used by the PKI of extant heterogeneous wireless networks. This algorithm deals with threshold cryptography BBN with a high level of security and availability. High ranked nodes with high equivalent power are nominated as servers and combiner nodes (BBN).

ACM-MANoN was evaluated using the NS-2 simulator, formal description and case studies.

The results of the evaluation confirm and prove that ACM-MANoN is a ***fully distributed*** security protocol that provides ***a high level of secure, available, scalable, flexible and efficient prevention*** management services for MANoN. Moreover, the applications of ACM-MANoN in military environments were also discussed.

9.2.3.2 BD-MANoN

BD-MANoN proposes a security protocol for managing digital certificates in a partially managed MANoN with non-defined elements in the MANoN environment. It combines both the certification authority characteristics of PKI and behaviour detection algorithm. The current research attempts to adapt one of these two approaches to MANoN. The proposed solution of BD-MANoN solves the shortcomings (engage of undefined elements) of ACM-MANoN and enhances the level of security by combining those features.

BD-MANoN was evaluated using a well-presented military case study. The results of the evaluation confirms that BD-MANoN is a ***fully distributed*** security protocol that provides ***a high level of secure, available, scalable, flexible, reliable and efficient detection*** management services for MANoN.

9.3 Achieving Success Criteria

To answer the research questions that we highlighted in Chapter 1, security solutions have been presented throughout the thesis in the form of: Firstly, *Security Architecture* providing end-to-end security solutions in order to predict and detect security vulnerabilities “Chapter 4”. Secondly, *Access Control* mechanism to prevent malicious nodes form gaining access to our MANoN system leading towards providing other security requirements such as data-confidentiality and data integrity “Chapter 6”.

Thirdly, a *Behavioural Detection* algorithm as a second line of defence in order to detect insider nodes trying to bring the MANoN system down “Chapter 7”.

9.4 Evaluation with Related Work

This section will highlight the advantages of our approach by drawing a meaningful comparison with other existing works in the ad hoc wireless technology. To recap on our achievements, a clear comparison with the security architecture based upon the standard X.805 in the ITU-T recommendation will be provided. As it can be seen in section 4.2 that our security architecture provides seven security requirements applied to four security layers and two security planes creating a logical division to a complex set of architecture components with eight proceeds which, makes applying security requirements more flexible. In the meantime, as shown in the recommendation X.805, the security architecture defines eight security dimensions with three security layers and three security planes creating nine proceeds in a tabular form making it more complex for users to apply the security requirements to such type of architectures.

Meanwhile, refereeing to our security algorithms (ACM-MANoN “Chapter 6” and BD-MANoN “Chapter 7”) providing a comparison with similar studies is irrelevant as our security mechanisms are an integration of different components (Security Administration, Prevention & Detection, and Containment and Recovery) not to mention, the state-of-the-art Mobile Ad hoc Network of Networks (MANoN), which is an integration of both ad hoc networks and network of networks.

9.5 Future Work

The following list highlights areas of research which are worth pursuing.

- ***Security architecture implementation:*** The full implementation of the security architecture presented in Chapter 4 guarantees an end-to-end security solution for MANoN. This thesis implements part of the security architecture by proposing two security algorithms for managing digital certificates in MANoN. These algorithms enforce the objectives of authentication, authorisation, availability, data confidentiality, data integrity and non-repudiation in proceeds (1), (2), (7) and (8). Therefore, there are still other possible mechanisms by which it would be possible to achieve the objectives of all security requirements in all proceeds. An interesting observation is that the security architecture has provided MANoN with a clear line of defence

- ***Security mechanism enhancements:*** Some of the future enhancements that can be made to the security mechanism BD-MANoN and its evaluation, provide a supported evaluation using the NS-3, which have all the detection components provided to implement the behaviour detection algorithm. Moreover, they can provide an Ana Tempura simulation and provide a comparison analysis between the results of NS-3 and Ana Tempura

- ***MANoN challenges:*** There are interesting challenges in a MANoN, in addition to security, which are worth investigation in future work. These include:

    - Multicast routing protocols design
    - MAC layer protocols development

- Efficient load balancing approaches
- End-to-End Quality of Service (QoS) provision
- Power-efficient protocol design
- Cross-layer design for wireless networks
- Multipath routing approach development
- Pricing schemes in MANoN

References

[1] N. Abramson, “Development of the ALOHANET”, *Information Theory IEEE Transactions*, Vol. 31, Issue 2, Mar 1985, pp: 119 – 123.

[2] Agency Research Project Agency (ARPA), http://www.apra.mil, last visited 15th November 2008.

[3] J. Al-Jaroodi, “Security Issues In Wireless Mobile Ad Hoc Networks (MANET)”, Technical Report TR02-10-07, University of Nebraska-Lincoln, 2002.

[4] A. H. Al-Bayatti, H. Zedan, and A. Cau, “Security Solution for Mobile Ad Hoc Network of Networks (MANoN)”, IEEE Fifth International Conference of Networking and Services ICNS 2009, pp. 225 – 262.

[5] E. Altman and T. Jimenez, “NS2 for beginners”, lectures notes 2003-2004, University of de Los Andes, France, 4th December 2003.

[6] N. Asokan and P. Ginzboorg, “Key-Agreement in Ad Hoc Networks”, Computer Communications, vol.23, no. 17, pp: 1627-1637, 2000.

[7] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, “An On-Demand Secure Routing Protocol Resilient to Byzantine Failures”, Proceedings of the ACM Workshop on Wireless Security 2002, pp. 21 – 30, September 2002.

[8] S. Basagni, , et al. “Secure Pebblenets“, In Mobile ad hoc networking & computing (MobiHOC 2001), Long Beach, CA, USA, 2001.

[9] M. Bechler, H. Hof, D. Kraft, F. Pahlke, and L. Wolf, “A Cluster-based Security Architecture for Ad hoc Networks”, INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, Volume 4, 7-11, pp.2393 – 2403, March 2004.

[10] S. Bellemo, and J. D. Smith, “Attributes of Effective Configuration Management for Systems of Systems”, System Conference 2008 2nd Annual IEEE, pp. 1 – 8, April 2008.

[11] A. Boukerche and Y. Ren, "A Security Management Scheme Using a Novel Computational Reputation Model for Wireless and Mobile Ad hoc Networks", Proceeding. PE-WASUN, 2008, pp.88-95.

[12] R. Boutaba, and A. Polyrakis, “Projecting FCAPS to Active Networks”, Enterprise Networking, Applications and Services Conference Proceedings, 2001 pp. 97 – 104, 2001.

[13] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad hoc Network Research", Wireless Communication & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, vol. 2, no. 5, pp. 483 – 502, 2002.

[14] E. Carrieri, C. A. Rpcchini, A. Fioretti, and A. J. Haylett, “An OSI Compatible Architecture for Integrated Multichannel Metropolitan and Regional Networks”, Integrating Research, Industry and Education in Energy and Communicational Engineering, MELECON '89, Mediterranean, pp.639 – 643, 11 – 13 April 1989.

[15] S. Capkun, J.-P. Hubaux, and Levente Buttyan, “Mobility helps security in ad hoc networks”, In Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003), June 2003.

[16] S. Capkun, J. P. Hubaux, and L. Buttyán, “Mobility Helps Peer-to-Peer Security”, IEEE Transactions on Mobile Computing, volumn 5, no. 1, pp: 43–51, Jan. 2006,.

[17] S. Capkun, L. Buttyan, and J.-P. Hubaux, “Self-organized public-key management for mobile ad hoc networks”, IEEE Transactions on Mobile Computing, 2(1), pp: 52-64, 2003.

[18] S. Capkun, L. Buttyan, and J. Hubaux, “Small Worlds in Security Systems: an Analysis of the PGP Certificate Graph”, Proceedings ACM New Security Paradigm Workshop (NSPW), 2002.

[19] P. Chandra, Bulletproof Wireless Security GSM, UMTS, 802.11 and Ad Hoc Security, Elsevier, 2005, ISBN: 0-7506-7746-5.

[20] Y. Chung, T. Chen, C. Liu, and T. Wang, “Efficient Hierarchical Key Management Scheme for Access Control in the Mobile Agent”, Advanced Information Networking and Applications – Workshops, 2008. AINAW 2008. 22nd International Conference, pp. 650 – 655, 25 – 28 March 2008.

[21] C. Chiang, G. M. and L. Zhang, “Adaptive shared tree multicast in mobile wireless networks”, Global Telecommunications Conference, GLOBECOM 98. The Bridge to Global Integration. IEEE , Vol. 3 , 8-12 Nov. 1998, pp:1817 – 1822.

[22] B. Dahill, B. Neil Levine, E. Royer and C. Shields, “A Secure Routing Protocol for Ad Hoc Networks“, Technical report UM-CS-2001-037, University of Massachusetts, Amherst, August, 2001.

[23] H. Deng, W. Li, and D. Agrawal, ”Routing Security in Wireless Ad hoc Networks”, IEEE Communications Magazine, Volume 40, Issue 10, pp. 70 – 75,2002.

[24] Defence Advanced Research Project Agency (DAPRA), available at http://www.darpa.mil, last visited 3rd December 2008.

[25] P. Dewan and P. Dasgupta, “Trusting Routers and Relays in Ad hoc Networks”, Proceedings of the 2003 International Conference on Parallel Processing Workshops (ICPPW’03), 2003.

[26] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, pp. 29 – 40, November 1976.

[27] J. R. Douceur, “The Sybil Attack”, Electronic Proceedings for the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), 2002.

[28] K. Donkyun, C.Toh, and C. Yanghee, “RODA: a new dynamic routing protocol using dual paths to support asymmetric links in mobile ad hoc networks Computer Communications and Networks”, Proceedings. Ninth International Conference on, 16-18 Oct. 2000, pp: 4 – 8.

[29] K. Fall, and K. Varadhan, “The ns Manual (formerly ns Notes and Documentation)”, The VINT Project, 13 December 2003.

[30] Y. Frankel, P. Gemmell, P. D. MacKenzie and M. Yung, “Proactive RSA“, In Proceedings of CRYPTO 1997, Springer Verlag LNCS, pp: 440–454, 1997.

[31] X. Fei, and W. Wenye, “Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks”, MILCOM 2006, Oct. 2006, pp. 1 – 7.

[32] K. Fokine, “Key Management in Ad Hoc Networks”, Master Thesis, Linkping University, 2002. http://www.liu.se/.

[33] S. Garfinkel, “PGP: pretty good privacy”, Minor corr. March 1995 ed., Beijing: O'Reilly & Associates. xxxiii, 393 p, 1995.

[34] M. Gerla, K. Tang, and R. Ragrodia, “TCP performance in wireless multi-hop networks”, Mobile Computing Systems and Applications, Proceedings. WMCSA '99. Second IEEE Workshop on, 25-26 Feb. 1999, pp: 41 – 50

[35] “Grep-GNU Project- Free Software Foundation (FSF)”, http://www.gnu.org/software/grep/, Last visited 20th December 2008.

[36] M. G. Gouda and E. Jung, “Certificate Dispersal in Ad-Hoc Networks“, IEEE Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS’04), 2004.

[37] “GloMoSim: Global Mobile Information System Simulation GloMoSim”, Home page, http://pcl.cs.ucla.edu/projects/glomosim/, Last visited 1st March 2007.

[38] S. Hayes, “A standard for the OAM&P of PCS systems”, personal Communications, Vol. 1, pp. 24 – 26, 1994.

[39] G. C. Hadjichristofi, W. J. Adams, and N. J. Davis IV, “A Framework for Key Management in Mobile Ad hoc Networks”, IEEE Proceedings of the International Conference on Information Technolgy: Coding and Computing (ITCC ’05), 2005.

[40] A. M. Hegland, S. F. Mjølsnes, C. Rong, Ø. Kure, and P. Spilling, “A Survey Of Key Management In Ad Hoc Networks”, IEEE Communications Surveys & Tutorials, Volume 8, Issue 3, pp:48 – 66, 2006.

[41] A. Hodjat and I. Verbauwhede, "The Energy Cost of Secrets in Ad-hoc Networks", IEEE Circuits and Systems Workshop on Wireless Communications and Networking, September 2002. Available at:
http://citeseer.ist.psu.edu/hodjat02energy.html , last visited 10th of December 2008.

[42] Y. Hu, A. Perrig, and D.B. Johnson, “Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad hoc Networks”, Proceedings of IEEE INFOCOM2003, vol.3, pp. 1976 – 1986, April 2003.

[43] L. Huang and T. Lai, “On the scalability of IEEE 802.11 ad hoc networks”, Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, June 2002, pp. 173 – 182, 2002.

[44] Y. Hu, A. Perrig, and D.B. Jonson, “Ariadne: A Secure On-Demand Routing for Ad hoc Networks”, Proceedings of ACM MOBICOM 2002, pp. 12-23, September 2002.

[45] G. Holland, and N. Vaidya, “Impact of routing and link layers on TCP performance in mobile ad hoc networks”, Wireless Communications and Networking Conference, WCNC. 1999 IEEE , 21-24 Sept. 1999, pp:1323 – 1327.

[46] Y.-C. Hu, D. B. Johnson and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks“, Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’02), Callicoon, New York, USA, June 20-21, 2002.

[47] H.Y. Hsieh, and R. Sivakmar, “Performance Comparison of Cellular and Multi-hop Wireless Networks: A Quantitative Study”, In Proceedings of ACM SIGMETRICS 2001, pp. 113–122, June 2001.

[48] Y. Hu, A. Perring, and D. B. Johnson, “Packet Lashes: A Defence Against Wormhole Attacks in Wireless Ad Hoc Networks”, Proceedings of IEEE INFOCOM 2003, vol. 3, pp. 1976-1986, April 2003.

[49] J. Hubaux, L. Buttyan, and S. Capkun, “The Quest for Security in Mobile Ad Hoc Networks“, In Mobile ad hoc networking & computing. Long Beach, CA: IEEE, 2001.

[50] E. Hyytiä and J. Virtamo, “Random waypoint model in n-dimensional space”, Operations Research Letters, vol. 33/6, pp. 567 – 571, 2005.

[51] J. Ironside, and L. J. Spencer, “Network Centric Warfare Operation in an Expeditionary Context”, Military information & Communications, symposium of South Africa (MICSSA), July 26, 2007.

[52] ITU-T Recommendation M.3010, “Principles for a Telecommunications management network”, February 2000.

[53] ITU-T Recommendation M.3400, “TMN Management Functions”, February 2000.

[54] ITU-T Recommendation X.509, *"Public-key and attribute certificate frameworks"*, August 2005.

[55] ITU-T Recommendation X.701, "Information technology - Open Systems Interconnection - Systems management overview", August 1997.

[56] ITU-T Recommendation X.800 (1991), "Security architecture for Open Systems Interconnection for CCITT applications", *1991*.

[57] ITU-T Recommendation X.805 (2003), "Security architecture for Systems providing end-to-end communications", 2003.

[58] ITU-T Recommendation M.3400 (02/2000), Telecommunication management network. Technical report, International Telecommunication Union- Telecommunication Standardisation sector (ITU-T), (02/2000).

[59] ITU-T Recommendation M.3400 (02/2000), Telecommunication management network. Technical report, International Telecommunication Union- Telecommunication Standardisation sector (ITU-T), 02/2000.

[60] IEEE Computer Society LAN MAN Standards Committee. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-1999, New York, 1999.

[61] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-hoc Wireless Networks", in Mobile Comput., T. Imielinski and H. Korth, Eds: Kluwer, 1996.

[62] S. Kurkowski, T. Camp, and M. Colagrosso, "MANET Simulation Studies: The Incredibles", ACM SIGMOBILE Mobile Computing and Communication Review, Vol. 9, Issue 4 October, 2005.

[63] A. Khalili, J. Katz, and W.A. Arbaugh, “Toward secure key distribution in truly ad-hoc networks“, Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT-w’03), 2003.

[64] O. Kachirski, and R. Guha, “Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks”, Knowledge Media Networking, 2002 IEEE Proceedings, pp. 153 – 157, 10 – 12 July 2002.

[65] S. Kurkowski, T. Camp, and M. Colagrosso, "MANET Simulation Studies: The Incredibles", ACM SIGMOBILE Mobile Computing and Communication Review, Vol. 9, Issue 4 October, 2005.

[66] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, “Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks”, International Conference on Network Protocols (ICNP), 2001.

[67] T. Ki, and O. K. Seong, “Cognitive Ad-hoc Networks under a Cellular Networking with an Interference Temperature Limit”, Advanced Communication Technology, Vol. 2, pp. 876 – 882, 17 – 20 February 2008.

[68] B. Lehane, L. Dolye and D.O. Mahony, “Ad hoc Key Management Infrastructure”, IEEE Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC ’05), 2005.

[69] H. Luo,*” Self-Securing Ad Hoc Wireless Networks”*, In IEEE symposium on computers and communications 2002, Taormina-Giardini Naxos, Italy: IEEE Computer Society, 2002.

[70] H. Luo and S. Lu. ”Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks”. Technical Report TR-2000. Available at: http://www.gta.ufrj.br/~eric/tese/artigos/TR200030.pdf, Last visited 1st December 2008.

[71] Y.D. Lin, and Y.C. Hsu, “Multi-hop Cellular: A New Architecture for Wireless Communications”, In Proceedings of IEEE INFOCOM, 2000, pp. 1273–1282.

[72] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, “URSA: Ubiquitous and Robust Access Control for Mobile Ad hoc Networks“, IEEE/ACM Transactions on Networking 12 (6) (2004), pp: 1049–1063.

[73] S. Levijoki, “Authentication, Authorization and Accounting in Ad Hoc networks”, Helsinki University of Technology, May 2000, http://www.tml.hut.fi/Opinnot/Tik-110.551/2000/papers/authentication/aaa.htm , Last visit on 1st November 2008.

[74] B. S. Manoj and C. Murthy, “Ad Hoc Wireless Networks: Issues and challenges”, Technical Report, Department of Computer Science and Engineering, Indian Institute of Technology, Madras, India, November 2003.

[75] A. H. Mohammed, H. Zedan, and A. Cau, “Security Architecture for MANoN”, Proceedings of the Forth International Conference on Networking of IDIAS 2008, April 2008.

[76] C. Murthy and B. S. Manjo, “Ad Hoc Wireless Networks: Architectures and Protocols”, Prentice Hall communications engineering and emerging technologies series Upper Saddle River, 2004.

[77] A. Mishra, K. Nadkarni, A. Patcha, and Virginia Tech, “Intrusion Detection in Wireless Ad Hoc Networks”, IEEE Wireless Communications, pp. 48 – 60, February 2004.

[78] A. Mishra and K. M. NadKarni, “Security in Wireless Ad Hoc Networks”, The Hand Book of Ad hoc Networks, CRC Press, FL, USA, 2003, pp. 479-490, ISBN: 0-8493-1332-5.

[79] P. Mohapatra, and S. Krishnamurth, “Ad Hoc Networks Technologies and Protocols”, Springer, 1 edition, September 23, 2004, pp: 1-3.

[80] M. Narasimha, G. Tsudik, and J.Yi, ”On the utility of distributed cryptography in P2P and MANETs: the case of membership control”, In Network Protocols, 2003. Proceedings. 11th IEEE International Conference on, 2003.

[81] National Institute of Standards and Technology (NIST), available at http://www.nist.gov/ , last visit on 26 October 2008.

[82] “North Atlantic Treaty Organization (NATO)”, Official homepage: http://www.nato.int /, last visit on 22nd March 2008.

[83] E. Ngai, and M.R. Lyu. “Trust- and Clustering-based Authentication Services in Mobile Ad hoc Networks“, 24th International Conference on Distributed Computing Systems Workshops, 2004, pp: 582-587.

[84] "OPNET Modeler" home page, http:// www.opnet.com/products /modeler/home.html, Last visited 19th December 2008.

[85] P. Papadimitratos and Z. J. Haas, "Secure Data Transmission in Mobile Ad hoc Networks", Proceedings of ACM Workshop on Wireless Security 2003, pp. 41 – 50, September 2003.

[86] PGPi.org, Documentation, "How PGP works", available at http://www.pgpi.org/doc/pgpintro/#p12 , last visit 2nd December 2008.

[87] R. Puttini, J. –M. Percher, L. Me, and R. De Sousa, "A Fully Distributed IDS for MANET", Proceeding of the Ninth International Symposium and Communication 2004 Volume 2(ISCC"04), Vol. 2, pp. 331 – 338, 2004.

[88] C.E. Perkins, and E.M. Royer, "Ad-hoc on-demand distance vector routing Mobile Computing Systems and Applications", Proceedings WMCSA'99. Second IEEE Workshop on, 25-26 Feb. 1999, pp: 90 – 100.

[89] K. Paul, R. Roy, and S. Bandyopadhyay, "Survivability Analysis of Ad Hoc Network Architecture", Proceedings of the IFIP-TC6/European Commission International Workshop on Mobile and Wireless Communication, Vol. 1818, pp. 31 – 46, 2000.

[90] C.E. Perkins, and E.M. Royer, "Ad-hoc on-demand distance vector routing Mobile Computing Systems and Applications", Proceedings. WMCSA'99. Second IEEE Workshop on, 25-26 Feb. 1999, pp: 90 – 100.

[91] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing”, (Internet-draft), in: Mobile Ad-hoc Network (MANET) Working Group, IETF, 17th February 2003.

[92] C.E. Perkins, and T.J. Watson, “Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers”, in: ACM SIGCOMM’94 Conference on Communications Architectures, London, UK, 1994.

[93] C. E. Perkins and E. M. Royer, “Ad Hoc On-Demand Distance Vector Routing”, Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999, pp. 90-100. February 1999.

[94] E. Royer, *“A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks”*, IEEE Personal Communication, April 1999.

[95] E. M. Royer, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, IEEE Personal communication, pp: 46 – 55, April 1999.

[96] K. Sanzgiri, B. Dahill, B. Neil Levine, C. Shields and E. Royer, “A Secure Routing Protocol for Ad Hoc Networks”, Proceedings of IEEE ICNP 2002, pp. 78 – 87, November 2002.

[97] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields and E. Beling-Royer. “A secure Routing Protocol for Ad Hoc Networks”. In proceedings of IEEE ICNP, 2002.

[98] A. Shamir, “How to Share a Secret”, Communications of ACM, 1979.

[99] B. Sun, K. Wu, Y. Xiao, and R. Wang, “Integration of Mobility and Intrusion detection for wireless ad hoc networks”, International Journal of Communication Systems, pp. 695 – 721, 2007.

[100] B. Schneier, “Applied Cryptography”, 2nd Edition, John Wiley & Sons, 1996, ISBN 0-471-11709-9.

[101] L. J. Spencer, and J. Ironside, “Network Centric Warfare Operation in an Expeditionary Context”, Military information & Communications, symposium of South Africa (MICSSA), 26 July 07.

[102] L. Stotts, S. Seidel, T. Krout, and P. Kolodzy, “MANET Gateways: Radio Interoperability Via the Internet, Not the Radio”, IEEE Communications Magazine, No. 6, Vol. 46, June 2008.

[103] W. Stallings, “Cryptography and Network Security: Principles and Practices”, 3rd Edition, Prentice Hall 2003, ISBN: 0-13-091429-0.

[104] W. Stallings, “Cryptography and Network Security: Principles and Practices”, 3rd Edition, Prentice Hall 2003, ISBN: 0-13-091429-0.

[105] S. Singh, and S. Raghavendra, “Power efficient MAC protocol for multihop radio networks”, Personal, Indoor and Mobile Radio Communications 1998, The Ninth IEEE International Symposium on, Volume: 1, 8-11 Sept. 1998, pp: 153 – 157.

[106] B. Tuch, “Development of WaveLAN an ISM Band Wireless LAN”, AT&T Technical Journal, 27–33, July/August 1993.

[107] C. Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems”, Prentice-Hall, New Jersey, pp: 34-37, 2002.

[108] C. Toh, V. Vassiliou, G. Guichal, and C. Shih, “MARCH: a medium access control protocol for multihop wireless ad hoc networks”, MILCOM 2000. 21st Century Military Communications Conference Proceedings, Volume: 1, 22-25 Oct. 2000, pp: 512 – 516.

[109] C. Toh, “Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks”, Communications Magazine, IEEE, Volume: 39, Issue: 6, June 2001, pp: 138 – 147.

[110] C. Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems”, Prentice-Hall, New Jersey, pp: 34-37, 2002.

[111] “Tcl Developer Xchange”, Main Tcl developer site, http://www.tcl.tk/, Last visited 1st March 2007.

[112] “The Network Simulator- NS-2”, Home page, http://www.isi.edu/nsnam/ns/, last visited 19th march 2008.

[113] T. Wen-Guey, “A secure fault-tolerant conference-key agreement protocol Computers”, IEEE Transactions on Volume 51, Issue 4, April 2002,pp. 373 – 379.

[114] Wikipedia.org, *"Man in the middle attack"*, available at: http://en.wikipedia.org/wiki/Man_in_the_middle , last visit on 26 October 2008.

[115] B. Wu, J. Wu, E. B. Fernandez and S. Magliveras, “Secure and Efficient Key management in Mobile Ad hoc Network”, Proceedings of the 19th IEEE International Prallel and Disributed Processing Symposium (IPDPS’05), 2005.

[116] H. Wu, C. Qiao, S. De, and O. Tonguz, “Integrated cellular and ad hoc relaying systems: iCAR”, IEEE Journal on Selected Areas in Communications 19 (10) (2001) pp. 2105–2115. 1994.

[117] G. Xu, and I. Liviu, “Locality Driven Key Management Architecture for Mobile Ad-hoc Networks”, Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference, 25-27 Oct. 2004, pp: 436 – 446.

[118] P. Yang, and S. Zheng, “Security Management in Hierarchical Ad Hoc Network”, Info-tech and Info-net, 2001. Proceedings. ICII 2001 - Beijing. 2001 International Conferences, Vol. 2, pp. 642 – 649, 29 Oct.-1 Nov. 2001.

[119] H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions”, IEEE Wireless Communications, 11 (1), pp: 38 – 47, 2004.

[120] S. Yi and R. Kravets, “MOCA: Mobile Certificate Authority for wireless ad hoc networks“, Proceedings of the 2nd Annual PKI Research Workshop (PKI 03), April 2003.

[121] S. Yi and R. Kravets, “Key Management for Heterogeneous Ad Hoc Wireless Networks”, Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP’02), 2002.

[122] S. Yi, P. Naldurg and R. Kravets, “Security-Aware Ad hoc Routing for Wireless Networks”, Proceedings of ACM MOBIHOC 2001, pp. 299-302, October 2001.

[123] Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks”, ACM Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[124] H. Zheng, S. Wang, and R. Nichols, “Policy-Based Security Management for Ad Hoc Wireless Systems”, Military Communication Conference, 2005, MILCOM 2005, IEEE, Vol. 4, pp. 2531 – 2537, 17 – 20 Oct. 2005.

[125] B. Zhu, F. Bao, R. H. Deng, Mohan S. Kankanhalli, and G. Wang, “Efficient and robust key management for large mobile ad hoc networks”, Computer Networks, vol 48, no. 4, July 2005, pp: 657-682.

[126] L. Zhou and Z.J. Haas, “Securing ad hoc networks“, Network, IEEE, 1999. 13(6): pp: 24-30.

[127] P. R. Zimmermann, “The official PGP user's guide”, Cambridge, Mass; London: MIT Press. xviii, 127p, 1995.