3-17-2006

Factors Impacting Key Management Effectiveness in Secured Wireless Networks

Yongjoo Shin

FACTORS IMPACTING KEY MANAGEMENT EFFECTIVENESS IN SECURED WIRELESS NETWORKS

THESIS

Yongjoo Shin, Captain, ROKA

AFIT/GIR/ENV/06M-09

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/06M-09

FACTORS IMPACTING KEY MANAGEMENT EFFECTIVENESS IN SECURED WIRELESS NETWORKS

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Yongjoo Shin, B.S.

Captain, ROKA

March 2006

AFIT/GIR/ENV/06M-09

FACTORS IMPACTING KEY MANAGEMENT EFFECTIVENESS IN SECURED WIRELESS NETWORKS

Yongjoo Shin, BS
Captain, ROKA

Approved:

Michael R. Grimaila, PhD (Chairman)	17 MARCH 2006 date
Kevin L. Elder, PhD (Member)	17 MAR 2006 date
Henry B. Potoczny, PhD (Member)	MARCH 17, 2006. date

Abstract

The security of ad hoc wireless networks has become a focal point of the military communications research community. A Mobile Ad Hoc Network (MANET) is an autonomous collection of mobile nodes that communicate over relatively bandwidth constrained, wireless links. Since MANETs require no existing communication infrastructure, they offer significant advantages in their scalability and flexibility. These attributes make MANETs extremely attractive for specialized application environments such as those encountered on the battlefield, in emergency situations, and in disaster areas. Unfortunately, MANETs also exhibit significant weaknesses in security when compared to other wireless communication solutions. They are subject to localized attacks and suffer from vulnerabilities inherent to their structure and topology.

The use of a Public Key Infrastructure (PKI) offers a cryptographic solution that can overcome many, but not all, of the MANET security problems. One of the most critical aspects of a PKI system is how well it implements Key Management. Key Management deals with key generation, key storage, key distribution, key updating, key revocation, and certificate service in accordance with security policies over the lifecycle of the cryptography. While traditional PKI solutions work well in fixed wired networks, they may not be appropriate for MANETs due to the lack of a fixed infrastructure to support the PKI. In this research, we investigate key management within PKI implementations in wireless networks to identify critical factors and best practices to secure these networks. Recommendations will be made for deploying secure MANETs based upon the research findings.

Acknowledgements

First of all, I would like to thank God for all of the blessings which he has given me and my family. I would like to thank my thesis committee, Dr. Michael R. Grimaila, Dr. Kevin L. Elder, and Dr. Henry B. Potoczny. Thank you for providing me invaluable suggestions and feedback on my research. Dr. Grimaila provided me support and encouragement that gave me the strength to complete my research even when I encountered difficulties. Despite my challenges with the English language, Dr. Grimaila helped me capture and refine my research findings in this thesis. I would thank the academic advisor who has always provided help and support from the day I arrived at AFIT. I would also like to thank all of my fellow GIR06M classmates for providing a positive and supportive community which made me feel at home.

Second, I would like to thank my loving wife and my new-born daughter for their support during these past eighteen months. They have willingly tolerated my absence during the many days and nights when I was busy working on his research. It is clear I could not have completed my research without their sacrifices.

Lastly, I would like to express my appreciation for my church family. They prayed for my family's safety and for the successful completion of my thesis. My church pastor and my pastor leader provided me with love and compassion. With their love, and the love of my family, I have been blessed by God and was able to complete my research.

Yongjoo Shin

Table of Contents

Page

Page

Page

List of Figures

Page

List of Tables

Page

FACTORS IMPACTING KEY MANAGEMENT EFFECTIVENESS IN SECURED WIRELESS NETWORKS

I. Introduction

1.1. Background

Advances in microelectronic technologies and reduced systems costs have resulted in the proliferation of low cost, wireless communication systems across a wide range of commercial and military communication solutions. In some cases, there is a need for the rapid deployment of independent mobile users working together towards a common goal. Examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. In many of these situations, cryptography may be employed to insure the confidentiality and integrity of the information carried in the network.

Key management is a fundamental part of any cryptography system used to secure a communications network. The effectiveness of a cryptography system largely depends on the security, robustness, and efficiency of the Key Management System. Specifically, Key Management deals with key generation, key storage, key distribution, key updating, key revocation, and certificate services, in accordance with security policies defined by the organization using the secure network (Bing, 2005).

A Key Management System (KMS) is the collective policy, practices, and procedures that are dictate the creation, distribution, and management of encryption keys. For this reason, the security and integrity of the KMS are fundamental aspects of a secure communications network (Hadjichristofi, 2005). An effective KMS provides high

service availability in distributed networks and requires minimal pre-configuration during the network deployment. Security services based on cryptographic mechanisms assume cryptographic keys to be securely distributed to the communicating parties otherwise the protection provided by the cryptography can be compromised. Secure key management is one of the most critical elements when integrating cryptographic functions into a system, since even the most elaborate security concept will be ineffective if the key management is weak.

A Mobile Ad Hoc Network (MANET) is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links (NISTMAN, 2005). One unique aspect is that the MANET is formed dynamically and will often employ a multi-hop routing communication scheme. Since the network topology may change rapidly and unpredictably over time, each node must incorporate a communication routing protocol that facilitates network discovery, insures message delivery, and detects and reroutes failed message delivery attempts. Since the networks are formed dynamically, each node should communicate with other nodes within its range and collect and distribute this information across the network. The major advantage of this type of network is the self-organizing property which eliminates the need for a fixed infrastructure found in other wireless-based networking solutions. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. Since MANETs are extremely flexible and scalable they are ideal for establishing communications in scenarios where there is no existing communications infrastructure.

Further, since the range of the communications network is limited, it appears to be an ideal solution for several military applications.

A security concern in wireless networks is that they are more readily prone to eavesdropping than a wired network, as there is no physical protection of the medium. Moreover, every node in MANET has increased responsibility in comparison to a node in a traditional fixed or mobile network because every node in MANET also serves as a router. The responsibility each node incurs increases the need for security measures to assure the confidentiality and integrity of each node. If a MANET node is compromised, it is possible it can act as a gateway to corrupt the entire network. Further, in some of the potential MANET application domain, such as those found in the military or law enforcement, security of the communications is a critical requirement. Moreover, even in conventional networks that do not require absolute confidentiality, the general public often demand privacy to keep their private information secure.

1.2. Problem Statement

With the rapid growth of Internet and wireless network technologies, many communication services have become the focus for future developments in the military operations, law enforcement, and disaster response domains. Since both Internet and wireless communications are transported over what is considered insecure transmission media, the messages have to be encrypted to prevent eavesdroppers or unauthorized users from capturing the messages. Therefore, secure communications has become a critical design factor when designing networks for the future (Tseng, 2003). However, there are

no established guidelines that identify best practices for deploying secure communications in new network topologies such MANET.

Security services based on cryptographic mechanisms assume cryptographic keys will be distributed to the communicating parties prior to secure communications. The secure management of these keys is one of the most critical elements when integrating cryptographic functions into a system, since even the most elaborate security concept will be ineffective if the key management is weak (Fumy, 1993). Key Management is the most critical factor of secure communication regardless of the application. Designing and implementing any kind of security mechanism requires a shared secret (usually called the cryptographic key) to construct a trust relationship between two or more communicating parties. Managing these cryptographic keys play a vital role in providing reliable, robust, and secure communication (Budakoglu, 2004).

Existing key management solutions are primarily developed based on conventional network topologies which are fixed and wired. In such networks, the infrastructure provided supports the underlying mechanisms required for effective key management. In contrast, wireless ad hoc networks by definition have no fixed infrastructure elements. Moreover, the nodes of wireless ad hoc networks, especially sensor network, have several limitations such as memory storage and computational capabilities. These inherent disadvantages make it difficulty to employ the tradition solution such as the solution based on a Public Key Infrastructure (PKI).

The nodes in a wireless ad hoc network are vulnerable to variety of potential attacks. An adversary only needs to identify and corrupt a single weak node to potentially

disrupt the whole network. One way to mitigate this threat is to implement a cryptographic solution with strong key management.

1.3. Research Question

The purpose of this study is to identify and assess existing key management techniques used to secure wireless communication network. The analysis will identify the strengths and weaknesses inherent in each of the key management techniques. This research will also identify critical factors related to key management that influence organizational acceptance of cryptography technology in secure communication network. It is believed that the identification of these factors will provide guidelines for the successful implementation of other wireless secure communications network such as MANET.

In order to satisfy the objective of this study, the primary research question is "What are the factors impacting Key Management effectiveness in secured wireless networks?" It is hoped that by answering this question, we can recommend guidelines and best practices for securing MANETs.

In addition, there are five investigative questions which allow us to effectively answer the primary research question.

1) What are the characteristics of various secure wireless communications?
2) What are the most common problems encountered when implementing a secure wireless network?
3) What are the critical success factors in deployment of a secure wireless network?
4) What are types of cryptography are used to secure wireless network?

5) What is the advantages/weakness of each cryptography technique?

1.4. Methodology

The research conducted in this thesis uses a hybrid research methodology. A content analysis research methodology is used to examine all literature related to secure network deployment and to compare and contrast the key characteristics of secure communication networks. A case study methodology is employed to examine secure network implementations in detail and to validate the key characteristics identified in the content analysis. Multiple databases will be queried in order to discover all relevant literature related to the key management aspects of securing wireless networks. Based on the collected and evaluated data, critical factors in key management impacting of the deployment of secure wireless networks will be identified. Finally, a comparative analysis of the each wireless network topology will be conducted in order to provide a better understanding of securing networks so that guidelines can be established for mobile ad hoc networks.

1.5. Scope and Limitations

The scope of this research study is the implementation of secured wireless communications. In this study, the range of secure communication networks examined includes wireless networks (WNs), wireless sensor networks (WSNs), and mobile ad-hoc networks (MANETs).

There are a number of limitations of this research. First, the implementation of the hybrid research methodology is problematic since I have both formulated the research

questions and conducted the categorization of references myself which introduces research bias. Second, there is a lack of substantial information available on MANET implementations. This is primary a consequence of the infancy of the MANET technology. Third, I am unable to obtain some of the classified references due to my status as an international student. Therefore, I will analyze all of the unclassified references related to securing wireless related network topologies and infer guidelines and best practices in MANETs. Finally, I will focus my research on Key Management issues rather than the underlying technical and mathematical details of the cryptography used in securing a network. This research will survey, provide an overview, and analyze the literature related to key management aspects of securing WNs, WSNs, and MANETs.

1.6. Thesis Overview

In this chapter, I have provided a brief introduction of the issues related to securing wireless networks. The remainder of the paper is organized as follows. Chapter 2 presents a literature review of all key management related secure wireless network literature. This chapter explains the basic concept of cryptography including key management in a secure communications environment. Chapter 3 describes the hybrid methodology used in this study in order to answer the research questions. In chapter 4, we provide a detailed analysis of Key Management techniques and discuss their implementation in a secure wireless communication network. Chapter 5 provides a detailed summary of the analysis conducted and provides conclusions and recommendations for future research.

II. Literature Review

2.1. Overview

In this chapter, we examine all existing literature related to securing wireless networks. The objective of this chapter is to provide common understanding of wireless network environment, security, and key management. This chapter will introduce the concept of a secure network, introduce the basic concepts of symmetric and asymmetric cryptography, and discuss the importance of a Pubic Key Infrastructure (PKI) and its relation to key management. The literature review provides the necessary background information to understand the importance of key management in a secured wireless network environment.

2.2. The Secured Wireless Communications Network Environment

2.2.1. Wireless Networks (WNs)

The future of communications has dramatically changed as the result of the deployment of low cost, wireless communications technology. The integration of wired and wireless networks has enabled new collaborative communication capabilities that link military sensors in theater with command and control systems located thousands of miles away. Large numbers of entities participating in these communications require the use of efficient methods of securing network in order to reduce network congestion (Kostas, 2003).

There has been a rapid development in high-speed computing and communication, miniaturization of computers, and deployment of wireless communication infrastructures. Today, Wireless Local Area Networks (WLANs) are rapidly and widely accepted as a complementary technology to high-speed wired LAN technologies and various cellular networks. WLANs have experienced an amazing development and a rapid growth. Advances in these technologies have engendered a new paradigm of computing providing flexibility in accessing information anywhere and at any time. For a wider acceptance, WLAN technologies should evolve such that they support QoS (Quality-of-Service) provisioning, secure communications, integration with other wireless networks, power conservation, seamless mobility support and a fair bandwidth sharing (Labiod, 2004).

In wireless networks, where the error rate is high and the bandwidth is limited, the design of key management schemes should focus on reducing the communication burden associated with key updating. A global wireless infrastructure will free users from the confines of static communication networks. Users will be able to access the Internet from anywhere at anytime. As wireless connections become ubiquitous, users will desire to have secure applications running on their mobile devices (Yan, 2004).

Network security has received critical attention from various areas. As the data network becomes more pervasive and its scale becomes larger, network intrusion and attacks have become larger threats to network users. This is especially true for the emerging wireless data networks. Compared to their wired counterpart, wireless networks are especially prone to security attacks ranging from passive eavesdropping to active interfering. It is difficult to protect against intrusions in the wireless environment and occasional intrusions in a large scale mobile network are inevitable over long periods

of time (Kong, 2001). Because of wireless links' specific characteristics, new security flaws arise within a WLAN. The necessity of securing WLANs has led to a consensus on the definition of newer, more robust authentication architectures. (Bakirdan, 2003).

2.2.2. Wireless Sensor Networks (WSNs)

As technology advances and the integration of low-power radio, computing and sensor technology becomes reality; wireless sensor networks (WSNs) are introduced as new type of wireless networks. These networks will typically consist of a lot of ultra low power nodes, with limited communication means and CPU power (Kahn, 1999; Rabaey, 2000).

Sensor networks consist of a large number of sensor nodes which typically have limited resources. They are used to monitor buildings and industries, and they can also be used in asset tracking, environmental sensing, etc. Generally, sensor nodes communicate with each other through wireless communication; therefore, security services such as encryption and authentication are required to prevent eavesdropping, alteration, and spoofing (Ito, 2005). In sensor network, there are many applications like gathering distributed information. Typically, the low-power sensors which scattered over the area to be monitored have the ability to gather data, and process and forward it to a central node for further processing (Jolly, 2003).

Wireless sensor networks (WSNs) consist of a large number of small sensor nodes equipped with limited computation capacity, restricted memory space, limited power resource and short-range radio communication device (Zhen, 2005). WSNs can be used in a wide range of applications, including military sensing, environment monitoring,

collecting vital signs of patients, smart houses, etc. Most of these applications require high-leveled security for WSN. WSN has its own characteristics, such as being prone to change; being limited in energy, memory and computation resources; and being subject to physical attack. These characteristics make it a challenging work to design secure scheme for WSN (RuiYing, 2005).

Although the capacities of these sensor nodes are growing, their resources are still very limited. In such an environment, overheads should be kept to a strict minimum, nodes should go into "sleep mode" to save energy, and security protocols should follow the same "energy-focused" design and consume as little power as possible (Seys, 2005).

In military applications, sensor nodes may be deployed in a hostile environment such as battlefield. Security is challenges for wireless sensor networks, because an adversary can easily gain access to mission critical or private information by monitoring communications between sensor nodes. For example, an adversary may try to eavesdrop on confidential traffic, to impersonate nodes to insert bogus data, and to cripple normal network operation by maliciously modifying routing information. In order to protect WSNs from these attacks, communication should be encrypted and authenticated. Therefore, it is important to encrypt communications between sensor nodes to maintain confidentiality (Zhen, 2005).

2.2.3. Mobile Ad Hoc Network (MANET)

Mobile ad hoc networks (MANET) are special type of wireless networks where mobile hosts in wireless network may form a temporary network without the aid of any fixed and centralized infrastructure. In a MANET, nodes within their wireless ranges can

communicate with each other directly, assuming that all nodes have the same transmission range. On the other hand, nodes outside the range have to use some other intermediate nodes to relay messages which create dynamic, multi-hop communication architecture. In such a communication, the packets sent by source host are relayed by several intermediate hosts before reaching the destination host (Bing, 2005). For this reason, every node plays a role of a router and must be capable of dynamically rerouting and storing messages on an as needed basis. In order for this network architecture to work, there must be a common protocol that all nodes use to achieve reliable communications.

In MANETs, the need for pre-existing infrastructure is not required because each of the nodes perform all network services. These nodes can communicate each other autonomously. The error-prone wireless medium and frequent link breakage caused by node mobility make the connectivity between the nodes to be irregular. A fully self-organized MANET allows the end-users to establish the network solely for a common purpose in an ad hoc fashions. For example, a group of strangers with computing devices who have never met before might create a self-organized MANET for a common purpose. These strangers have no pre-existing relationships and share no common secret keying material on their nodes. Thus, users within this network have to establish security associations between themselves after the network is constructed without any aid of a pre-shared keying material or any form of trusted third party (Merwe, 2005).

Low resource availability demands efficient resource utilization and makes it difficulty to use complicate authentication and encryption algorithms. Most often, limited power storage and computational capability prevent nodes in MANETs to utilize

enhanced encryption methodologies. Conventional PKI-based authentication and encryption mechanisms are relatively expensive in computational power to generate and verify digital signatures. This cost often prevents their practical application to use in MANETs. Symmetric key technique has been proven to be more efficient due to less computational complexity, but comes with the cost of pre-sharing a secret key (Deng, 2004).

One of the main goals of this research is to determine if traditional PKI-based cryptography is suitable for used in MANETs. The inherent infrastructureless nature of MANETs makes it hard to provide the capability required in traditional PKI implementations. In addition, another serious problem that occurs in MANETs is the physical vulnerability of the nodes themselves. While mobile nodes within an infrastructure-based wireless networks have the same vulnerability, they easily receive some help with recovery since they can rely on the infrastructure for detection and remediation of compromised nodes. In an infrastructure-based network, infrastructure has most sensitive information which mobile nodes need in order to communicate and the mobile nodes manage only minimal information. In a MANET, the mobile nodes have a higher vulnerability profile since there is no stable infrastructure (Yi, 2002).

Many target applications for MANETs require strong communication security to operate. Prime examples include battlefield communication support, law enforcement communications, and disaster recovery operations which bring together large communities of diverse organizations. However, the same infrastructureless nature of MANETs that makes it ideal for easy, fast, and cost-effective deployment also makes it difficulty to support secure communications. Many security solutions rely on public key

(asymmetric) cryptography, the deployment of which requires the effective management of digital certificates through two fundamental services: secure binding of a cryptographic key to an entity (e.g. a user, a mobile node, or a service) and the validation of such bindings to other entities. Most key management frameworks and other security services designed for wired networks and infrastructure-based wireless networks rely on a trusted infrastructure for security-related functions. However, in an ad hoc network without any infrastructure support, most traditional solutions are not directly applicable (Yi, 2004).

MANETs are a new paradigm of wireless communication for mobile nodes. In a MANET, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Figure 1 shows such an example: initially, nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken. However, the network is still connected, because A can reach D through C, E, and F. Military tactical operations are still the main application of ad hoc networks today. For example, military units (e.g., soldiers, tanks, or planes) equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and disaster recovery missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms (Zhou, 1999).

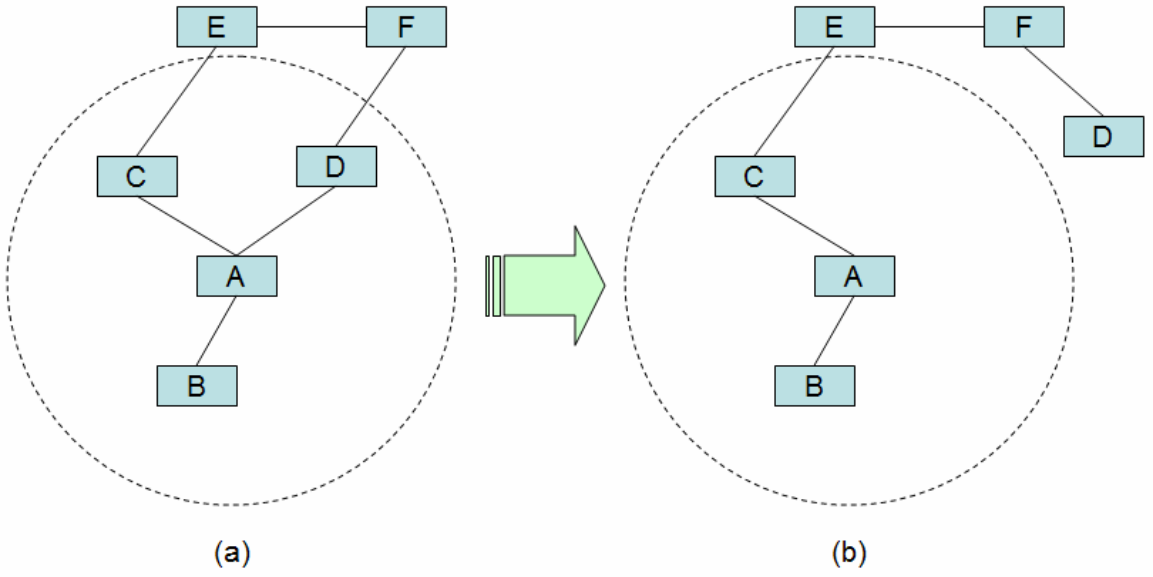

Figure 1. Ad Hoc Mobile Networks (Zhou, 1999)

Topology change in ad hoc network: nodes *A*, *B*, *C*, *D*, *E*, and *F* constitute and ad hoc network. The circle represents the radio range of node *A*. The network initially has the topology in (a). When node *D* moves out of the radio range of *A*, the network topology changes to the one in (b).

Wireless ad hoc networks have been proposed to support dynamic scenarios where no wired infrastructure exists (Yi, 2001). Most ad hoc routing protocols are cooperative by nature (Royer, 1999), and rely on implicit trust-your-neighbor relationships to route packets among participating nodes. This naïve trust model allows malicious nodes to paralyze an ad hoc network by inserting erroneous routing updates, replaying old routing information, changing routing updates, or advertising incorrect routing information (Marti, 2000). While these attacks are possible in fixed networks as well, the nature of the ad hoc environment magnifies their effects, and makes their detection difficult (Zhang, 2000).

Ad hoc networks are subject to various kinds of attacks. Wireless communication links can be eavesdropped on without noticeable effort and communication protocols on all layers are vulnerable to specific attacks. In contrast to wire-line networks, known attacks like masquerading, man-in-the-middle, and replaying of messages can easily be carried out. Moreover, deploying security mechanisms is difficult due to inherent properties of ad hoc networks, such as the high dynamics of their topology (due to mobility and joining/leaving devices), limited resources of end systems, or bandwidth-restricted and possibly asymmetrical communication links (Bechler, 2004).

2.3. Symmetric vs. Asymmetric Cryptography

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is considered the science of protecting information by encoding it into an unreadable format for later decryption only by authorized parties. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through untrusted network communication paths (Harris, 2003)

Cryptography techniques are used to enable secure communications in both wired and wireless networks (Bing, 2005). Symmetric key cryptography has computation efficiency, but it also has weaknesses in the management of secret keys. Asymmetric key cryptography is widely used because of its simplicity in key distribution. However, this technique relies on a centralized infrastructure and is resource expensive.

In symmetric key techniques, the sender and recipient have pre-shared a secret key, which is used for various cryptographic operations, such as encryption, decryption and verification of message authentication data (Dankers, 2002). Thus, parties who want to

communicate each other have the same secret key in order to encrypt and decrypt messages. This secret key must be exchanged in a separate out-of-band procedure prior to the intended communication. The need to exchange a secret key prior to the intended communication complicates the security for transactions between entities that do not have a pre-established relationship. Authentication is provided by proving possession of the pre-shared secret key to each other. As the number of keys grows, the administration and management of secret keys, including their generation, distribution, renewal and storage, can become intractable. For each pair of entities, a secret key has to be created and distributed, so that for a group *n* entities communicating with each other $\frac{n(n-1)}{2}$ keys are required (Dankers, 2002). Figure 2 shows that the number of key required in symmetric key cryptography system grows exponentially with the number of users.

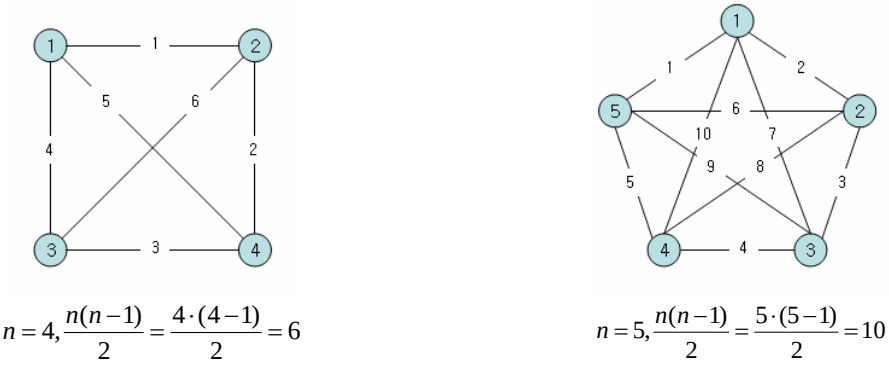

Figure 2. The Number of Keys Required in Symmetric Cryptography

Because of the need for pre-shared secret keys, secret key based solutions scale poorly. However, a major advantage of symmetric secret key techniques is that they are computationally efficient and they require small overhead when compared to asymmetric

key techniques (Dankers, 2002). This is the main reason why many applications currently still use secret key mechanisms for communication system. Figure 3 demonstrates the process of symmetric key cryptography.

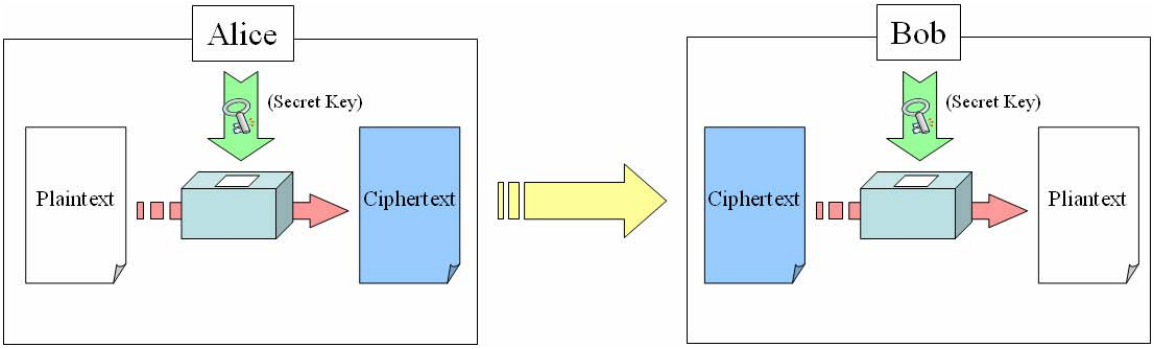

Figure 3. A Symmetric Key Cryptography System

Symmetric key cryptography performs encryption and decryption with a single key. The security of this system is thus determined by protecting the "secret key" from disclosure. As such, this is applicable only in situations where the distribution of the key can occur in a secure manner. Many applications often preclude the "safe" distribution of the key, and so symmetric-key cryptography is often used in tandem with asymmetric cryptography. Examples of symmetric cryptography algorithms include DES, 3DES, Blowfish, IDEA, CAST128, and Arcfour.

An asymmetric key technique is used for public key cryptography system (Dankers, 2002). Usually each user has just one key pair consisting of a public key and a private key. One of the keys of the pair is made publicly available, while the other key is kept private. Because one of the keys is available publicly there is no need for a pre-shared secret key. Note that restricting distribution of the public key can be used to enable

secure communications between organizations who may want to share information securely in the future. However, there is a need for an infrastructure to distribute and manage the public key authentically. Because there is no need for pre-existed secrets prior to a communication, public key techniques are appropriate for supporting security between previously unknown parties such as ad hoc network. Authentication is achieved by proving possession of the private key (Dankers, 2002). A digital signature is one mechanism used for doing this. The digital signature is generated with the private key and verified using the corresponding public key, which is bound to the entity generating the signature (Dankers, 2002).

Asymmetric key techniques make it possible to establish secret keys dynamically (Dankers, 2002). In simplified procedure, an end-entity calculates a secret key and sends it encrypted with the public key of the entity with which it wants to communicate. That entity then obtains the secret key by decrypting the received information with its private key. As the public key of a key pair is usually published in a directory, the overhead associated with distributing key material to communicating parities is reduced significantly in comparison with solutions based solely on symmetric secret key techniques. For a group of *n* entities communicating with each other, only *n* key pairs are required (Dankers, 2002). However, a weakness of asymmetric key techniques is that they are computationally very intensive. This intensiveness makes them less suitable for environment where devices of size and processing power are limited, such as wireless sensor network. Figure 4 demonstrate the process of asymmetric key cryptography.

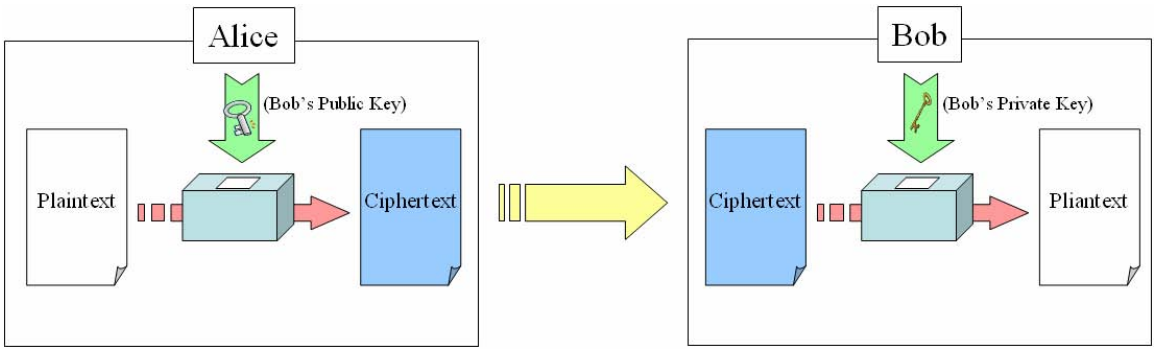

Figure 4. An Asymmetric Key Cryptography System

In asymmetric cryptography, the public and private keys are related to each other, but obtaining the private key from its public counterpart is an NP-complete problem and is thus infeasible to undertake. To illustrate how public-key cryptography works, consider the hypothetical example of two people named Alice and Bob who would like to communicate with each other in private. Assuming Alice already has Bob's public key, she encrypts her message to Bob with his public key. Bob receives the message and decrypts it using his private key. If an eavesdropper, say Eve, were to capture Alice's message in transit and re-send it to conceal her presence, she will be unable to decrypt it just by owning a copy of Bob's public key. She can certainly try to obtain the private key from the public key but it will take her a prohibitively long time to do so. RSA and DSA are examples of public key cryptographic algorithms.

2.4. Public Key Infrastructure (PKI)

Public key cryptography is one of most effective mechanisms for providing fundamental security services including authentication, digital signatures and encryption for the successful implementation of asymmetric key cryptography (Yi, 2002). Public

Key Infrastructure (PKI) provides a means for key management and the infrastructure necessary for managing digital certificates. The most important component of PKI is the CA (Certificate Authority), the trusted entity in the system that vouches for the validity of digital certificate. The success of PKI depends on the availability of the CA to the principals in the system (or the nodes in the network) since a principals must correspond with the CA to get a certificate, check the status of another principal's certificate (in some cases), and acquire another principal's digital certificate. PKI is widely used in wired networks and some infrastructure-based wireless networks (Yi, 2002).

Public key cryptography is uniquely well-suited to certain parts of a secure global network. It is widely accepted that public key security systems are easier to administer, more secure, less trustful, and have better geographical reach, than symmetric key security systems. However, it is not widely appreciated that these advantages rely excessively on the end-user's security discipline. With public key cryptography, clients must constantly be careful to rigorously validate every public key they use, and they must maintain the secrecy of their long-lived private keys. It turns out that these tasks are harder than they seem (Davis, 1996).

The ubiquitous capability of verifying the binding between a public key and the owner principal plays an important role in the successful application of pubic key cryptography. In a communications system, the mainstream solution is to have a third-party centrally trusted entity, called Certificate Authority (CA), vouch for the authenticity of the binding by signing digital certificates. In practice, CAs and digital certificates are organized and maintained by the standards defined by the Public Key Infrastructure. In a wireless environment, all devices are opened to attack to the same extent and no one can

be assumed to be significantly more secure than the others. Moreover, devices can roam, run out of power, leave and later rejoin a network, stop functioning, all of which lead to volatile connectivity among nodes and CAs (Gang, 2004).

A Public Key Infrastructure (PKI) consists of program, data format procedures, communication protocols, security policies, and public key cryptographic mechanisms working in a comprehensive manner to enable a wide range of dispersed people to communicate in a secure and predictable fashion. In other words, a PKI establishes a level of trust within an environment. Formally, a PKI is an ISO authentication framework that uses public key cryptography and the X.509 standard protocols. The framework was set up to enable authentication to happen across different networks and the Internet. Particular protocols and algorithms are not specified, which is why PKI is called a framework and not a specific technology (Harris, 2003).

Many security protocols in use today were designed under the assumption that some form of global distributed public-key infrastructure would eventually emerge to address key management problems. These protocols go back to the early 1990s, when a universal PKI was thought to be available in the short term. Unfortunately, it has not evolved as quickly as thought. Consequently, existing protocols originally designed to rely on a global PKI must either employ ad hoc solutions (Gutmann, 2004).

2.4.1. Certificate Authority

PKI architectures traditionally fall into three configurations: A single CA, a hierarchy of CAs, or a mesh of CAs. Each configuration is characterized by the number

of CAs, the trust relationships between the CAs, and where PKI users place their trust (Polk, 2003):

- **Single CA**: The simplest architecture contains a single CA that provides certificates and certificate status information for every user. The CA's public key is the fundamental point of trust, or trust anchor, for evaluating certificate acceptability. Users have a direct relationship with the CA, so they know which applications the certificates should be used for.
- **CA Hierarchy**: PKIs constructed with superior–subordinate CA relationships are called hierarchical PKIs. The foundation of such an architecture is the "root" CA (the trust anchor for all users of the PKI), which issues certificates to subordinate CAs but not to users.
- **CA Mesh**: The traditional alternative to hierarchical PKIs is to create a mesh PKI, or web of trust, to connect CAs via P2P relationships. Any CA in a mesh PKI can be a trust anchor, although users generally consider the CA that issued their certificate as their trust anchor.

2.4.2. Algorithm

A standard analogy (Mollin, 2003) for public-key cryptography is given as follows. Suppose that Bob has a wall safe with a secret combination lock known only to him, and the safe is left open and made available to passers-by. Then anyone, including Alice, can put messages in the safe and lock it. However, only Bob can retrieve the message, since even Alice, who left a message in the box, has no way of retrieving the message.

The key-exchange protocol devised by Diffie-Hellman (Diffie, 1976) did not provide a complete solution to the notion give above of a public-key cryptosystem. The first to publicly do this were Rivest, Shamir, and Adleman (RSA), for which their name are attached to the cryptosystem which we now describe.

We break the algorithm into two parts with the underlying assumption that Alice wants to send a message to Bob. The first part is RSA key generation.

(1)	Bob generates toe large, random prime $p \neq q$ of roughly the same size.
(2)	He computed both $n = pq$ and $\phi(n) = (p-1)(q-1)$. The integer *n* is called hi s (RSA) modulus.
(3)	He select a random $e \in N$ such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. The int eger *e* is called his (RSA) enciphering exponent.
(4)	Using the extended Euclidean algorithm, he computes the unique $d \in N$ with $1 < d < \phi(n)$ such that $ed \equiv 1 (\mathrm{mod}\, \phi(\mathrm{n}))$
(5)	Bob publishes (*n, e*) in some public database and keeps *d, p, q,* and $\phi(n)$ priva te. Thus, Bob's (RSA) public-key is (*n, e*) and his (RSA) private key is d. the i nteger d is called his (RSA) deciphering exponent.

Table 1. First Part of RSA Algorithm (Mollin, 2003)

The second part is RSA public-key cipher. This part again is dived into two subparts; enciphering stage and deciphering stage. In enciphering stage, in order to simplify this stage, we assume that the plaintext message $m \in M$ is in numerical form with $m < n$. Also, $M = C = Z / nZ$, and we assume that $\gcd(m, n) = 1$.

(1) Alice obtains Bob's public-key (*n, e*) form the database.
(2) She enciphers *m* by computing $c \equiv m^e \pmod{n}$ using the repeated squaring m ethod.
(3) She sends $c \in C$ to Bob.

Table 2. Second Part of RSA Algorithm (Mollin, 2003)

In deciphering stage, once Bob receives c, he used d to compute $m \equiv c^d \pmod{n}$. Moreover, the decryption is unique in that we always recover the intended plaintext.

2.5. Key Management

Cryptography can be used as a security mechanism to provide confidentiality, integrity, and authentication as long as the keys are not compromised in any way. If the keys can be captured, modified, corrupted, or disclosed to unauthorized individuals, then the whole cryptosystem can become compromised. Cryptography is based on a trust model. Individuals trust each other to protect their own keys, they trust the administrator who is maintaining the keys, and they in turn trust a server that holds, maintains, and distributes the keys.

Key management is a basic part of any secure communication. Most cryptosystems rely on some underlying secure, robust, and efficient key management system. Key management deals with key generation, storage, distribution, updating, revocation, and certificate service, in accordance with security policies. If the key is exposed, the encrypted information would not be protected from malicious attacker. The secrecy of the symmetric key and private key must be guaranteed assuredly. Key distribution and key agreement through an insecure channel is at high risk and suffers

from possible attacks. In the traditional digital envelop approach, one side produce a session key and encrypts it using the public-key algorithm. After such a generation and encryption, the other side receives and recovers it. In the Diffie-Hellman (DH) scheme, communication parties of both sides share some public information and generate a session key on both sides. A number of complicated key exchange or distribution protocols and frameworks have been designed and built. However, mobile ad hoc networks have strongly restricted computation load and complexity of key agreement protocol because of node's lack of available resource, dynamic network topology, or network synchronization difficulty. Key integrity and ownership should be protected from strong key attacks. Digital signature, message digest and hashed message authentication code (HMAC) are techniques used for the data authentication or integrity purpose. In the same way, public key is protected by public-key certificate in which a trusted entity called certification authority (CA) in PKI vouches the binding of the public key with owner's identity. In systems where there is no trusted third party (TTP), public-key certificate is vouched by peer nodes in a distributed manner, such as pretty good privacy (PGP). Obviously, the purpose of key authentication is that certificate can prove the ownership of key rather than decide whether it is good or not. After certain valid period of usage, the key could be compromised or disposed. Since key should not use again after its disclosure, some mechanism is required to revoke the compromised key in not expired period. Certificate contains the lifetime of validity. If the key is expired, it is not useful. However, the private key maybe is able to be disclosed during the valid period. In this case, certificate authority (CA) needs to revoke this certificate explicitly and notify

the network by using the certificate revocation list (CRL) to prevent its invalid usage (Bing, 2005).

Key maintenance is a very important factor in securing a communications network. There is more to key maintenance than simply using them to encrypt and decrypt messages. The keys have to be distributed securely to the right entities and updated continuously. The keys need to be protected as they are being transmitted and while they are being stored on each workstation and server. The keys need to generated, destroyed, and recovered properly on demand by authorized individuals. The keys must be stored securely before and after distribution. When a key is distributed to a user, it is not going to be located in any location; it needs a secure place to be stored and used only in a controlled manner. The keys, the algorithm that will use the key, configurations, and parameters are stored in a module that also needs to be protected. If an attacker were able to obtain these components, she could masquerade as another user and decrypt, read, and re-encrypt messages that were not intended for her (Harris, 2003)

A Key Management System (KMS) creates, distributes, and manages these certificates. Thus, the KMS is at the heart of the network's defenses. A KMS provides high service availability in highly partitioned networks, requires minimal pre-configuration during the network deployment phase, and can accommodate new nodes joining the network (Hadjichristofi, 2005).

Cryptographic keys have to be randomly generated. The secret keying material that must either be physically secured or enciphered allows protecting itself from disclosure, and the authentication of keying material prevents from illegal modification. Authentication may be implemented with the use of parameters like counters or

timestamps to also protect from replay of old keys, insertion of false keys, and substitution or deletion of keys. All keying material is related to one or more subjects/objects of a system. Additionally it intended to be used for some particular purpose. A major threat for systems is generated when proper identification of all subjects accessing the system is provided. Thus, a key management system is feasible if it guarantees the relation between an entity and its uniquely defined keys (Fumy, 1993).

If the key management has weakness, the security system using this cryptography is ineffective. Key management is the most important element of secure communication network. The secrecy of the cryptographic key is essential when designing and implementing any kind of security mechanism in order to set up a trust relationship between two or more communicating parties. Managing these cryptographic keys play a critical role in establishing reliable and robust security communication. Key management can be defined as generating, storing, distributing, deleting or archiving keys in reference to a security policy (Budakoglu, 2004).

Key management activities include the generation, distribution or agreement, storage, utilization, archiving, deletion, and destruction of cryptographic key material to support cryptographically based security mechanisms employed by security protocols. Because OSI is concerned solely with the communications aspects of end-system and intermediate systems, a key management protocol is limited to the communications aspects of key management. An implementation of an OSI key management protocol and its supporting security mechanisms must ensure that key material is not disclosed or modified during exchanges, and that the key material is protected from insertion, substitution, and deletion (Jansen, 1993).

The level of security provided by an encryption-based scheme for secure communication across a data network is highly dependent on the security of the keys used for the encryption and decryption of data. The feasibility of such an updating, particularly when end-to-end encryption is contemplated, depends on the existence of a key management mechanism that facilitates, at the initiation of each new session, the generation of a session key and its distribution to the two end communicants. Furthermore, it is desirable that this transfer be made on the existing communication channels, which in turn demands the highest level of security during such a transfer. Consequently, key management is more important to the working security of a network than the mathematical structure of the encryption algorithm itself, since an inefficient key transfer between the end communicants can make the entire scheme worthless regardless of how complex the encryption itself is (Lu, 1989).

2.5.1. Key Exchange

Key exchange is the most primitive form of key management. People wishing to communicate over an insecure channel must exchange a cryptographic key. The use of physical key exchange was the earliest form of key management, if it can be described as key management at all. Usually, key exchange is the most inconvenient method of creating a secure association between two communicating entities. However, in some ad hoc networking scenarios it is NOT inconvenient but actually a requirement. Thus, for small personal area networks or similar scenarios, physical key exchange must be both logical and convenient (Lehane, 2003).

2.5.2. Key Agreement and Group Keying

Group keying allows multiparty secure communications, and hence provides group level authentication and security. However, providing keying information for individual members of the group (i.e. to allow people to communicate privately in the presence of other group members) requires other predetermined key agreements. Indeed networks may form where group affiliation doesn't exist, particularly in a large-scale civilian network. As such, a group key agreement is of limited utility in a non-group oriented network, such as a civilian network in which many nodes choose to communicate but some require end-to-end privacy. A public key infrastructure is better suited to this scenario (Lehane, 2003).

2.5.3. A Summary of Key Management

A summary of key management is provided below (Bing, 2005):

1. The secrecy of key itself must be assured in the local host system.
2. Secured network communications involved in the key distribution procedure between communication parties must be insured when the key may be transmitted through insecure channels to maintain key confidentiality and integrity.
3. A framework of trust relationships needs to be built for authentication of key ownership. While some frameworks are based on a centralized Trusted Third Party (TTP), other could be fully distributed. For example, a Certificate Authority is the TTP in PKI, Key Distribution Center (KDC) in the symmetric system, meanwhile in PGP, no such a trusted entity is assumed.
4. The key can become expired or have been revoked within its valid period.

III. Methodology

3.1. Overview

This chapter discusses the methodologies used to conduct this research. In order to answer the primary research question, both a content analysis and a case study methodology are employed. In some cases, a qualitative approach may be used. Finally, a comparison analysis is provided in last stage in order to offering better understanding of results. Specifically, this chapter will describe the research design, explain why the methodology approach is appropriate for this effort, and describe how these data will be analyzed to answer the research question presented.

3.2. Selecting Methodology

Leedy (2001) provides a methodology to select between the Qualitative and Quantitative research approaches. Leedy (2001) also enumerates five basic research characteristics: purpose, process, data collection, data analysis, and reporting findings. These characteristics help the researcher to make a decision so that best approach applies to their particular area of study. In Table 3 (Leedy, 2001), there are five general questions used to determine if the research is quantitative or qualitative.

Question:	*Quantitative*	*Qualitative:*
What is the purpose of the research?	• To explain and predict • To confirm and validate • To test theory	• To describe and explain • To explore and interpret • To build theory
What is the nature of the research process?	• Focused • Known variables • Established guidelines • Static design • Context-free • Detached View	• Holistic • Unknown variables • Flexible guidelines • Emergent design • Context-bound • Personal view
What are the methods of data collection?	• Representative, large sample • Standardized instruments	• Informative, small sample • Observations, interviews
What is the form of reasoning used in analysis?	• Deductive analysis	• Inductive analysis
How are findings communicated?	• Numbers • Statistics, aggregated data • Formal voice, scientific style	• Words • Narratives, individual quotes • Personal voice, literary style

Table 3. Selection of Methodological Approach (Leedy, 2001)

1) Purpose: Quantitative researchers seek to explain and predicate relationships and to develop generalizations. Qualitative researchers seek a better understanding and may use their observations to build theory (Leedy, 2001).

2) Process: Leedy (2001) also discusses the research process. The quantitative research processes provides carefully structured guidelines. The qualitative research process is more holistic and emergent in design, measurement instruments, and interpretations (Leedy, 2001).

3) Data Collection: Leedy (2001) states that during quantitative data collection, researchers identify variables and accumulate data specifically related to those variables

from a population. In qualitative data collection, the researchers operate under the assumption that reality is not easily divided into discrete, measurable variables.

4) Data Analysis: For data analysis, all research requires logical reasoning. Quantitative researchers tend to depend on deductive reasoning while qualitative researchers make considerable use of inductive reasoning. (Leedy, 2001).

5) Report Findings: In order to report findings, quantitative researchers typically reduce their data numbers and employ the power of interpretation. Qualitative researchers construct interpretive narratives from their data and try to capture the complexity of the phenomenon under study (Leedy, 2001).

By using these questions to determine the proper research approach, the qualitative methodology appears to me the most desirable methodology for this research. Leedy (2001) explains that research studies are enhanced by combining both qualitative and quantitative research approaches. Even if quantitative approach is not designed, this study may use some quantitative data that may enhance the qualitative data analysis.

On the other hand, Yin (2003) states, there are several ways for social science research. These consist of: experiments, surveys, histories, analysis of archival information, and case study. When choosing a research method, each strategy has advantages and disadvantages, depending on three conditions: (a) the type of research question, (b) the extent of control an investigator has over actual behavioral events and (c) the degree of focus on contemporary as opposed to historical phenomena (Yin, 2003). Table 4 shows these three conditions and explains how to be related to the five major research strategies.

Strategy	Form of Research Question	Requires Control of Behavioral Event?	Focuses on Contemporary Events
Experiment	How, Why?	Yes	Yes
Survey	Who, What, Where, How many, How much?	No	Yes
Archival analysis	Who, What, Where, How many, How much?	No	Yes / No
History	How, Why?	No	No
Case Study	How, Why?	No	Yes

Table 4. Strategy for Research Design (Yin, 2003)

3.3. Qualitative Research

The qualitative study is an inquiry process of understanding a social or human problem conducted in a natural setting. The three factors determine the appropriate research approach: research problem, personal experiences of the researcher, and the audience. The qualitative approach is appropriate to investigate exploratory research problems by researchers with experience in literary writing and intending to present their results to practitioners (Creswell, 2003).

In addition, other researchers provide guidelines for selecting the qualitative approach. According to Leedy (2001), a case study is a type of qualitative research in which information is collected about a single or multiple cases to learn more about an unknown or poorly understood state of affairs (Leedy, 2001). Yin state that case studies investigate contemporary problems within real-life context to account for pertinent influences on the research topic (Yin, 2003).

Leedy (2001) explains that the relationship between data and methodology is inextricably interdependent. For this reason, choosing the appropriate methodology must always consider the data that will be collected in the resolution of the problem. To accurately state, the research questions, a flexible approach was needed to explore the unknown. Patton (2002) explains that qualitative inquiries come from exploration, discovery, and inductive logic. An inductive approach is used in this research to find out what the important questions and variables are (Patton, 2002). Then, a qualitative approach is suitable to answer the research and investigative questions of this exploration.

Quantitative research is used when exploring the relationships between measured variables in order to explain, predict, or control phenomena (Leedy, 2001). Moreover, quantitative research tries to either prove or disprove hypotheses that are under study. Conversely, qualitative research attempts to answer questions relating to the complexity of a phenomenon using the participant's point of view as the basis for explaining or understanding the events (Leedy, 2001). Lastly, qualitative research may end with hypotheses generated or temporary answers relating to the phenomena under study. The qualitative research methodology is used in a lot of disciplines in an attempt to determine and explain what has happened or is happening (Leedy, 2001).

A qualitative approach is appropriate when developing new insight about a phenomenon (Leedy, 2001). In the case of this research, the phenomenon is the environment of secure network such as mobile ad hoc network and the insights are the security issues on such a secure network. Because the data for this research is obtained from written text, Denzin categorize it as a test as proxy for experience using free flowing

text (Denzin, 2000). They list six methodologies that could be used for this type of data, but suggest content analysis as the most appropriate research method for this type of data (Denzin, 2000). Leedy (2001) agrees with this description of content analysis as a detailed and systematic examination of the contents of a particular body of material for the purpose of identifying patterns (Leedy, 2001). By analyzing text, the researcher finds codes or the intent of what is written (Leedy, 2001). Neuendorf (2002) also concurs by stating that a content analysis is a systematic, objective, quantitative, analysis of message characteristics. Each of these definitions shows that content analysis is an appropriate methodology in order to satisfy the purpose of this research. Thus, content analysis was chosen as the best methodology to answer the questions posed in this study.

3.4. Case Study

The case study is especially suitable for learning more about a poorly understood situation (Leedy, 2001). The case study strategy is used when the research satisfies the following three conditions: the research questions must be in the form of how or why, the researcher must not have any control over events, and the study must focus on a contemporary event or problem (Yin, 2003).

Yin (2003) defines the appropriateness of case study as a research method by providing the following technical definition: A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident (Yin, 2003).

Leedy (2001) also supports the use of a case study in situations when its unique or exceptional qualities can promote understanding or inform practice for similar situations,

and a case study may be especially suitable for learning more about a little known or poorly understood situation (Leedy, 2001).

A number of definitions for the case study methodology have existed over the years. In case studies, the researcher explores in depth a program, an event, an activity, a process, or one or more individuals. The case (or cases) is bounded by time and activity. Researchers gather detailed information using a variety of data collection procedures (Stake, 1995).

The case study approach to qualitative research constitutes a specific way of collecting, organizing, and analyzing data (Patton, 2002). In a case study, a particular individual, program, or event is studied in-depth for a defined period of time (Leedy, 2001). The researcher will investigate a topic when the theory base is unknown (Creswell, 2003). The researcher tries to test the validity of certain assumptions, claims, theories, or generalizations within real-world contexts (Leedy, 2001).

A lot of the definitions of case study exist (Leedy, 2001; Patton, 2002; Stake, 1995; Yin, 2003). Yin (2003) states that the case study constructs an all-encompassing method and it include the logic of design, data collection techniques, and specific approaches to data analysis. Regardless of the chosen definition, Benbasat (1987) explain that the case study is suitable to capture the knowledge of practitioners and to develop theories. Benbasat (1987) listed eleven characteristics of case studies. Table 5 is the eleven characteristics. These characteristics of the case study method were related to the purpose of this research.

1. Phenomenon is examined in a natural setting.
2. Data are collected by multiple means.
3. One or few entities (person, group, or organization) are examined.
4. The complexity of the unit is studied intensively.
5. Case studies are more suitable for the exploration, classification and hypothesis development stages of the knowledge building process; the investigator should have a receptive attitude towards exploration.
6. No experimental controls or manipulation are involved.
7. The investigator may not specify the set of independent and dependent variables in advance.
8. The results derived depend heavily on the integrative powers of the investigator.
9. Changes in site selection and data collection methods could take place as the investigator develops new hypotheses.
10. Case research is useful in the study of "why" and "how" questions because these deal with operational links to be traced over time rather than with frequency or incidence.
11. The focus is on contemporary events.

Table 5. Key Characteristics of Case Studies (Benbasat, 1987)

A case study is an ideal methodology when a holistic, in-depth investigation is needed (Feagin 1991). The case study is preferred in examining contemporary events, but only when the relevant behaviors cannot be influenced (Yin 2003). Case studies are designed to bring out the details from the viewpoint of the participants by using multiple sources of data (Tellis 1997).

3.5. Comparison Analysis

In final stage of completing this study, a comparative analysis of the usability of guidelines created from the qualitative literature review will be performed. Patton (2002) states, that understanding unique cases can be deepened by a comparative analysis. Comparisons can also be important in illuminating differences between programs in evaluation (Patton, 2002). In this study, the key management strategy used in each secure network environment will be compared and analyzed to determine 1) which is better then others, 2) if one is abstractly secure, and/or 3) if one has good characteristics in particular environment will it satisfy the requirements of the others.

3.6. Content Analysis

3.6.1. Definition of Content Analysis

Content analysis is a research technique for making replicable and valid inferences from texts (or other meaningful matter) to the contexts of their use. As a technique, content analysis involves specialized procedures. It is learnable and divorceable from the personal authority of the researcher. As a research technique, content analysis provides new insights, increases a researcher's knowledge of particular phenomena, or informs practical actions (Krippendorff, 2004).

3.6.2. Advantages of Content Analysis

Compared with other data-generating and analysis techniques, content analysis has several advantages (Weber, 1990):

1. Communication is a central aspect of social interaction. Content analytic procedures operate directly on text or transcripts of human communication.
2. The best content analysis studies use both qualitative and quantitative operations on texts. Thus content analysis methods combine what are usually thought to be antithetical modes or analysis.
3. Documents of various kinds exist over long periods of time. Culture indicators generated form such series of documents constitute reliable data that may span even centuries.
4. In more recent times, when reliable data of other kinds exist, culture indicators can be used to assess quantitatively the relationships among economic, social, political, and cultural change.
5. Compared with techniques such as interviews, content analysis usually provides unobtrusive measures in which neither the sender nor the receiver of the message is aware that it is being analyzed. Hence, there is little danger that the act of measurement itself will act as a force for change that confounds the data.

3.6.3. Issues in Content Analysis

A central idea in content analysis is that the many words of the text are classified into much fewer content categories. Each category may consist of one, several, or many words. Words, phrases, or other units of text classified in the same category are presumed to have similar meanings. Depending on the purposes of the investigator, this similarity may be based on the precise meaning of the words, or may be based on words sharing similar connotations. To make valid inferences from the text, it is important that the

classification procedure be reliable in the sense of being consistent. Different people should code the same text in the same way. Also, the classification procedure must generate variables that are valid. A variable is valid to the extent that it measures or represents what the investigator intends it to measure (Weber, 1990).

3.6.4. The Nine Step Process of Content Analysis

In the content analysis methodology, the researcher identifies the specific material to be analyzed and how to precisely code that material (Leedy, 2001). Then the researcher uses quantitative analysis techniques to a matrix of these coded entries to construct the central themes across the data (Denzin, 2000). Neuendorf (2002) suggests the nine step process. Table 6 briefly explains these steps.

1. Theory and rationale: *What* content will be examined, and *why*? Are there certain *theories* or perspectives that indicate that this particular message content is important to study? Library work in needed here to conduct a good literature review.

↓

2. Conceptualizations: What *variables* will be used in the study, and how do you define them conceptually? There are many way to define a given construct, and there is no one right way.

↓

3. Operationalizations: Your measure should match your conceptualizations. What *unit of data* collection will you use? An *a priori* coding scheme describing all measures must be created. Both face validity and content validity may also be assessed

↓

4. Coding schemes: You need to create the following materials.

a. *Codebook* (with all variable measure fully explained)
b. Coding form

↓

5. Sampling: is a census of the content possible? How will you *randomly sample* a subset of the content? This could be by time period, by issue, by page, by channel, and so forth.

↓

6. Training and pilot reliability: During a training session in which coders work together, find out whether they can agree on the coding of variables.

↓

7. Coding: Use at least two coder, to establish intercoder reliability. Coding should be done independently, with at least 10% overlap for the reliability test.

↓

8. Final reliability: Calculate a reliability figure for each variable.

↓

9. Tabulation and reporting: See various examples of content analysis result to see the ways in which results can be reported. Figures and statistics may be reported one variable at a time, or variables may be cross-tabulated in different ways.

Table 6. A Flowchart for Content Analysis Research (Neuendorf, 2002)

3.7. Research Design

3.7.1. Theory and rationale

This step explains what references will be examined and why they are selected. The focus of the content analysis is to include all of the articles related to key management in secure wireless network. The reference materials will be collected using various sources. Generally, the intentions of the researcher can cause certain references to be included or excluded, which can be the source of significant bias. In order to reduce this bias in the reference selection process, the references are chosen randomly (Leedy, 2001).

3.7.2. Conceptualizations

This step describes what variables will be used in the research and how they will be conceptualized (Neuendorf, 2002). In order to answer the research questions, each of the secure wireless network environments including the Wireless Network (WNs), Wireless Sensor Network (WSNs), and Mobile Ad Hoc Networks (MANETs) are explained. The basic concepts of cryptography used in each of the wireless networks are described to provide insight into how the network is secured. The review chapter provides an explanation of the Public Key Infrastructure which is the most effective mechanism process for implementing Key Management.

3.7.3. Operationalizations

In this step, the unit of measure employed in this research is defined. This unit of measure is important to provide the code schemes (Neuendorf, 2002). This research used

the reference article as the unit of measure. In order to reduce researcher input into selecting process, there is no weight and no bias based on the author or source. However, since the primary researcher could not examine all of the related references, only a subset of all possible references was used in this research.

3.7.4. Coding schemes

The coding scheme is used to analyze and categorize the data. Once all relevant references are identified, the references will be coded to indicate if they provide information on the characteristics of wireless networking and/or key management in a secured wireless network. The words used in searching are “key management”, “security”, and “cryptography”. In order to decide whether this is related to our key issue, the three codes are employed, as follows:

0 Not mentioned – the issue is not mentioned at all in the material

1 Mentioned - the issue is merely mentioned in the material

2 Key Idea – the idea is fully developed and is the focus of the paper

From this analysis, the list of important related issues were generated and stored. These issues were used by the research coders in order to analyze the material. The researcher analyzed and assessed the existence of these issues contained in the key issue list in the selected literatures.

3.7.5. Sampling

Since it is impossible to execute a complete census of the reference population, a random selection process was provided to collect data used in the content of the research (Neuendorf, 2002). In order to identify Key Management issues in secured wireless networks, a subsample of all related available literatures will be collected. The primary source of material for this study will be obtained from the Association for Computing Machinery (ACM; http://www.acm.org/) and Institute of Electrical and Electronics Engineers (IEEE; http://www.ieee.org/portal/site). In addition, the online research database in the AFIT Academy Library (http://www.afit.edu/library/) will be used to identify other significant resources to be used in this research.

For each reference, the title and abstract of the material are examined. If this material includes the concepts related to the research, the reference is read in its entirety. If the material is relevant, the reference is classified into wireless network (WNs, WSNs, and MANETs), key management (WNs, WSNs, and MANETs).

3.7.6. Training and pilot reliability

This section explains the role of research coders in performing their analysis. In this research, the research coders did not exist. Ideally, several coders are required in order to provide the reliability. Due to the limitations of obtain volunteers who have enough background related to wireless networks, security, and cryptography to evaluate and assess the data, this content analysis was conducted by only the primary researcher.

3.7.7. Coding

From the references related to general key management, the problem and critical issues of Key Management are examined and stored. These issues are recorded using the tool such as Microsoft Office Excel 2003. These issues were numbered, (e.g. Factor-1, Factor-2, … / Problem-1, Problem-2, …) While the selected are examined, if the ideas related to issues is found, the number of the issues are counted in the spreadsheet of Microsoft Office Excel 2003. The counted numbers of each issue are analyzed and interpreted in order to identify the main problems and factors of Key Management in each secure wireless network.

3.7.8. Final reliability

To make valid inferences from the text, it is important that the classification procedure be reliable in the sense of being consistent: different people should code the same text in the same way (Weber, 1990). Comparing the result of the primary researcher with ones of several coders provide the measure of reliability in validating the results. Since there are no coders to validate the results in this research, it is not possible to obtain the measure of reliability. However, this research attempted to obtain the key issues from a variety of references in order to examine various authors' opinions related to Key Management.

3.7.9. Tabulation and reporting

In the final step, the results of the study are tabulated and reported (Neuendorf, 2002). The final resulted were stored and arranged in the spreadsheet of Microsoft Office

Excel 2003. These results were transferred into pie chart in order for displaying them visually. These findings will be interpreted and discussed in chapter IV and chapter V.

3.8. Research Limitations

The results of this study are subject to limitations based upon constraints encountered in the research process. First, as with all qualitative research, the researcher plays a major role as key instruments in this study (Leedy, 2001). As a result, the intent of researcher can drastically have an effect on the research results in a lot of ways. This bias of researcher includes some issues such as researcher background, previous knowledge, personal predispositions, researcher skill, and competency (Leedy, 2001). Because of importance of researcher's role, it is impossible to completely remove all bias. In order to reduce this effect, all researchers should have an indirect position when conducting their analysis. Consequently, reducing researcher bias and choice is significant factor to provide good results. Unfortunately, in this study the author both formulated the research questions and conducted the content analysis without additional help in coding references.

Second, there is no way to perfectly obtain all written material concerning the key management in a secured network environment. There is limited and restricted factor to explore the related field in conducting this research. This issue must be considered when the researcher makes conclusions from these results (Leedy, 2001). Further, there is very little literature available about MANETs in general that contains substantial information about key management.

Third, some of the references that discuss securing wireless networks are classified and unavailable to an international student. This may result in some newer developments not being included in this research.

Finally, an inability to generalize the findings and results is another limitation of this research. This research targets only wireless network environment and does not attempt to generalize to other network environment. Thus, the guideline provided by this research may not be suitable for combined network environment and new wireless network environment which is not defined by this research.

IV. An Analysis of Key Management

4.1. The Secure Network Environment

4.1.1. Overview

In this study, we focus our attention on secure wireless networks. Specifically, our scope is limited to wireless networks (WNs), wireless sensor networks (WSNs), and mobile ad hoc network (MANETs). In order to present the characteristics of each secure network environment, a content analysis comprised of fifty-six salient documents was conducted. A list of references is contained in Appendix A.

4.1.2. Wireless Networks (WNs)

Characteristics (Advantage)

Wireless networks are being deployed ubiquitously at a remarkable pace. Low cost, ease of operation, platform independence, and product variety make them appealing to everybody (Godber, 2002). Wireless Local Area Networks (WLANs) will facilitate ubiquitous communications and location independent computing in restricted spatial domains. The main attractions of wireless network include: cost effectiveness, ease of installation, flexibility, tether-less access to the information infrastructure, and support for ubiquitous computing through station mobility (Park, 1998).

Schmidt (2003) explains the characteristics of WLANs as requiring zero configurations, ubiquity, and the ease of the creation of mesh networks. Karnik (2005) identified and demonstrated the financial and performance benefits of WLANs:

- Financial benefits: Intel Corporation conducted an analysis concluding that wireless networks offer significant savings in two financial areas such as Total Cost of Ownership (TCO) and Return on Investment (ROI).
- Performance benefits: Wireless networks also offer performance benefits in terms of increased accuracy and productivity

The IEEE has specified various WLAN standards, some of which are summarized below in Table 7 (Schmidt, 2003):

Standard	Description	Application
802.11a	• 5 GHz • 12 Channels • 22 Mbps	• Large-scale corporate environment • Less interference • Higher performance
802.11b	• 2.4 GHz • 3 Channels • 11 Mbps	• Hot Spots & Residential environment • Lower speed • Low cost & Variety of products
802.11g	• 2.4 GHz • 3 Channels • 54 Mbps	• Compatible with 802.11b • Higher speed

Table 7. Wireless Local Area Network Standard (Schmidt, 2003)

Weakness

Wireless networks provide convenience and low-cost deployment. However, they lack any inherent means of strong security (Allen, 2002). The standards committee for wireless network left many difficult security issues such as key management and a robust authentication mechanism as open problems. The fact that wireless networks provide a network access point for an adversary creates critical security problem. The end-to-end problem (easy access) affects wired as well as wireless security. However, it is much greater threat in wireless network because the attacker has easy access to the transport medium (Arbaugh, 2003).

A wireless network can be as secure as a wired network if security guidelines are implemented and enforced strictly. One of the major problems to provide secure network environment in wireless network is that wireless media are inherently less secure (Bharghavan, 1994). Security over a wireless environment is more complicated than in a wired environment. Due to the wide open nature of wireless radio, many attacks could make the network insecure (Chen, 2005).

Due to the nature of a wireless network, wireless communication is unprotected and can easily be eavesdropped on or even spoofed (Eisinger, 2005). Since in wireless LANs the bandwidth and the computing resources are limited, complex cryptographic protocols such as those requiring extensive computations and transmissions can not be considered (Park, 1998).

The Wired Equivalent Privacy (WEP) protocol was designed to provide confidentiality for network traffic using the wireless protocol. However, when WLANs was released, WEP was mistaken as an encryption solution. WEP was only designed to

provide wired-equivalent privacy on a wireless network. A wireless solution that uses WEP works in conjunction with another security system to provide the authentication and accounting necessary. Even in those situations, WEP does not perform the encryption necessary to consider a wireless network secure. Open source and freeware programs are easily available that crack and decode WEP sessions. Universities provide ideal incubators for such network subversion (Allen, 2002).

4.1.3. Wireless Sensor Networks (WSNs)

Characteristics (Advantage)

A sensor is a miniature device capable of detecting environmental conditions such as temperature, sound, humidity, seismic tremors, or the presence of certain objects. Sensors incorporate sensing, low-power data processing, and low-power wireless communication capabilities (Olariu, 2005). Wireless Sensor networks is an emerging paradigm of computing and networking where a node may be self-powered, and have sensing, computing, and communication capabilities (Bai, 2004).

The main driving forces for wireless sensor networks are fault tolerance, energy gain and spatial capacity gain. A wireless sensor network provides a suitable interface for interaction, physical control, information harvesting and exchange (Bilstrup, 2003). In sensor networks, it has many advantages to replace cables with wireless logical links. Its key features are robustness, low complexity, low power and low cost. A restriction of a position to set up sensor nodes disappears and it has more advantages to maintain, mend and recover than the existing wired network (Choi, 2004).

Being characterized by their low-power, small size, and cheap price, sensor nodes are capable of wireless communication, sensing and computations (Dai, 2005). Wireless sensor nodes have emerged as a result of recent advances in low-power digital and analog circuitry, low-power RF design and sensor technology (Rajaravivarma, 2003). Wireless sensor network have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicated in short distances. Sensor networks are highly vulnerable to security attacks (Tie, 2005).

Weakness

Remote wireless sensor networks are vulnerable to malicious attacks. While wired and infrastructure-based wireless networks have mature intrusion detection systems and sophisticated firewalls to block these attacks, wireless sensor networks have only primitive defenses. Wireless networks require innovative medium access techniques to share the limited broadcast bandwidth in a fair and efficient manner as computing and communications devices continue to proliferate (Brownfield, 2005).

One of the major barriers to deploying security on sensor networks is that current sensor devices have limited computation and communication capabilities. They are vulnerable to attacks which are more difficult to launch in the wired domain. Sensor networks are vulnerable to resource consumption attacks (Karlof, 2004). These sensors are inexpensive, low-power devices. As a result, they have limited computational and communication resources (Perrig, 2002).

When sensors are deployed in a hostile place like a battlefield, they are subject to physical attacks by an adversary. The adversary may be able to undetectably take control

of a sensor and compromise the cryptographic keys. The amount of key-storage in each sensor is highly limited; it is not capable to store keys with every other sensor. Typical sensor network platforms have very low bandwidth. Transmission reliability is often low, making the transmission of large blocks of data particularly expensive (Chen, 2005).

4.1.4. Mobile Ad Hoc Networks (MANETs)

Characteristics (Advantage)

An ad hoc WLAN has no ability to communicate with external networks without using additional routing protocols (Housley, 2003). Mobile ad hoc networks are infrastructure-free, pervasive, and ubiquitous without any centralized authority (Alampalayam, 2005). Ad hoc networks characteristics (dynamic topology, infrastructureless. variable capacity links. etc.) are origin of many issues (Bouam, 2003). The most important characterizing feature of a MANET is the absence of any node in a central role (Manikopoulos, 2003).

Interest in ad hoc networks largely stems from the ability to rapidly deploy them under both normal and harsh conditions. These networks can be quickly deployed in situations where no infrastructure exists and it would be impractical or infeasible to deploy infrastructure. In such an infrastructure-less network, nodes are expected to cooperate to perform essential networking tasks such as routing (Aboudagga, 2005).

Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed (Hu, 2002). The mobile ad hoc networks have several salient

characteristics: Dynamic topologies, Bandwidth-constrained, Variable capacity links, Energy constrained operation, Limited physical security (Yi, 2004).

Weakness

The lack of a clear line of defense and traffic concentration points poses a challenge to deploying security solutions in ad hoc networks. The broadcast nature of the transmission medium and the dynamically changing topology add even more complications. Furthermore, the reliance on node collaboration as a key factor of network connectivity presents another obstacle (Aboudagga, 2005). Ad hoc network routing protocols are challenging to design, and secure ones are even more so. The protocols also have high communication overhead because they send periodic routing messages even when the network is not changing (Hu, 2002).

MANETs bring great challenges in security due to its high dynamics, link vulnerability, and complete decentralization (Jiang, 2004). Major challenge is that of the compromised node(s); this could be an overtaken attacked node or a physically captured node (Manikopoulos, 2003). Ad hoc networks can be highly dynamic since wireless nodes are free to move about. Furthermore, wireless nodes have limited battery life and computational power to face these challenges (Suen, 2005). The problem is challenging due to the lack of centralized management/monitoring component, error-prone multi-hop wireless communication, and dynamics in the network topology (Yang, 2002). The ad hoc networks are susceptible to attacks due to wireless links, energy constraints, and difficulty to self-configure because of the mobility (Xie, 2004). Table 8 explains various types of attacks possible on a MANET (Aboudagga, 2005).

Method	Type of attack				Open Issues
	Authentication	Routing	Selfish	DoS	
GDH (Capkun, 2003)	Yes	No	No	No	Mechanism for certificate issues
MOCA (Yi, 2002)	Yes	Yes	No	No	Does not use the support of PKI
CORE (Michiardi, 2002)	No	No	Yes	No	Considers only selfish node attack
Nuglets (Buttyan, 2003)	Yes	Yes	Yes	No	Scheme is not generalized
CONFIDANT (Buchegger, 2002)	No	Yes	Yes	No	Assumes nodes are authenticated
Guardian Angel (Avoine, 2002)	Yes	No	Yes	No	Does not support varied attacks
TIARA (Ramanujan, 2000)	Yes	Yes	No	Yes	Not a generalized scheme
SEAD (Hu, 2002)	Yes	Yes	No	Yes	Packet forwarding
Beacon (Binkley, 2001)	Yes	Yes	No	No	Scalability and Key Management
SOS (Yang, 2002)	Yes	Yes	No	Yes	Scalability issues
SRP (Papdimitratos, 2002)	Yes	Yes	No	Yes	Unfair utilization of resources
ARIADNE (Hu, 2002)	Yes	Yes	No	Yes	Not optimized
SAR (Yi, 2002)	Yes	Yes	No	No	Packet mistreatment attacks
OSRP (Awerbuch , 2002)	Yes	Yes	No	No	Fixed but not adaptive threshold
WatchDog/ Pathrater (Marti, 2000)	No	Yes	No	No	Assumes no a priori relationship

Table 8. Summary of Different Types of Attacks on a MANET (Aboudagga, 2005)

4.1.5. Summary

Table 9 shows the advantage and weakness of each network environment. Wireless networks (WNs) have infrastructure which support stronger security than other wireless networks. Wireless sensor networks (WSNs) have sensor nodes with limited resources, which provide low cost and easy installation, and restricted computation capabilities. In mobile ad hoc networks (MANETs), there is no infrastructure. Although this enables MANETs to be pervasive and ubiquitous, it creates a number of security problems. These characteristics provide useful background information in order to construct and design secure wireless networks.

	Advantage	Weakness
WN	Ubiquitous deployment, low-cost, easy operation, dependent platform (computing), flexibility , financial and performance benefits	- The bandwidth and the computing resources are limited. - These natures of wireless network make the system to be less secure.
WSN	Robustness, self-powered, low-power, low-cost, easy maintenance	Vulnerability to malicious attacks, requirement of innovative medium , limited computational and communication resources
MANET	- No need of additional routing protocol and dynamic topology - Infrastructure-free, pervasive, and ubiquitous without any centralized authority	- The lack of a clear line of defense and traffic concentration points - High communication overhead - Great challenges in security due to its high dynamics, link vulnerability, and complete decentralization

Table 9. Advantage and Weakness of Secure Networks

4.2. Key Management Problems

4.2.1. Overview

In order to identify key management in existing secure network deployments, twenty-eight references (see Appendix B) related to key management were identified and examined. In this section, we will detail the problems identified in Key Management. Additionally, I identified fifty-six references which discuss key management in of each secure network type in detail. A content analysis of the references is conducted and discussed to identify the critical factors which affect the success of Key Management in secure wireless network implementations from related 56 documents (See Appendix C).

4.2.2. Key Management Problems

One central problem of key management is key distribution, i.e., the problem of establishing keying material whose origin, integrity, and-in the case of secret keys-confidentiality can be guaranteed. The problem with the concept of trust is that there is no formal understanding of it. The amount of trust required of course depends to some extent on the type of key management server (Fumy, 1993). Key management, in general, can be a difficult problem because of issues as: Distribution of keys; Distribution of lists containing revoked keys; Tracking which keys were valid during what period of time (Witzke, 1994).

A weak tie between a key and its owner invites Man In The Middle (MITM) attacks, which may succeed if the system can't distinguish communications with an intended recipient from those with the intervening attacker (Gutmann, 2004).

When the number of services one has to access increases, key management becomes a serious problem due to the fact that each membership-based service has a different secret token and the memory space on each card is very limited (Harn, 1993). Public key cryptography generally consumes lots of resources such as computation and communication, which is not believed suitable for pervasive computing due to the limited capabilities of pervasive devices (He, 2005). Furthermore, some of the key management protocols being standardized are single purpose, intended for a specific OS1 layer (Jansen, 1993).

All key-recovery systems require the existence of a highly sensitive and highly available secret key or collection of keys that must be maintained in a secure manner over an extended time period. These systems must make decryption information quickly accessible to law-enforcement agencies without notice to the key owners. These basic requirements make the problem of general key recovery difficult and expensive—and potentially too un-secure and too costly for many applications and many users (Neumann, 1997). The key-management problem mainly concerns minimizing the cost of key update communications and key storage requirements (Tseng, 2003).

Key management remains the primary obstacle to the wide-scale use of cryptography (Reiter, 1996).With symmetric systems, the movement of keys from place to place obviously must be done securely and with a level of protection adequate to counter the threats of concern to the using parties. The private keys are usually self-generated, but they may also be generated from a central source, such as a corporate security office. If all secure communications take place within the same corporation or

among locations under a common line of authority, key management is an internal or possibly a joint obligation (Dam, 1996).

4.2.3. Result and Analysis

The problems we identified in key management identified are summarized in Table 10 below.

1. Key distribution and the concept of trust
2. Weak relationship between keys
3. Different secret scheme
4. Limited memory storage and resource
5. Insufficient standard of key management
6. Difficult and expensive key recovery
7. Increasing cost of key management
8. Difficulty to apply wide-used cryptography

Table 10. The Problems of Key Management

Throughout a majority of references, the authors state that main problem is the distribution of the secret key. Most cryptography systems use the concept of key in order to support security. In a symmetric key system, parties to communicate with each other have pre-shared key. In addition, the public key is known to everyone in order to join the network using asymmetric key cryptography. While a wired network is supported by strong secure infrastructure, it is difficult for wireless networks to be as strongly secured. Thus, it is required to provide effective key distribution in deploying security wireless network.

Table 11 and Figure 5 illustrate how many references focus on each of the identified problems. Fifty-six references related to the key management problem were identified. Subsequently, they were divided into three categories: WNs, WSNs, and MANETs. Seven references were related to WNs, twenty-one references were related to WSNs, and twenty-eight references were related to MANETs. In all wired network references, the key distribution problem was identified. In all wireless network references key distribution, limited resources, insufficient and weak relationship standardization were identified. In wireless sensor networks (WSNs), key distribution, different secret scheme, limited resources, and key recovery were identified. MANETs references primarily deal with key distribution and increasing cost or key management.

In Table11, WNs have a greater occurance of problems 1, 4, and 5 than any other network. This means that key distribution, limited resources, and insufficient standard are main problems in WNs. WSNs have a greater occurance of problems 1, 3, and 6 than any other network. This means that key distribution, different secret scheme, and difficult key recovery are main problems in WSNs. MANETs have a greater occurance of problem 1 and 7 than any other network. This means that key distribution and increasing cost are main problems in MANETs. In all of three wireless networks, the key distribution is a main problem in deploying secure network. Figure 5 graphically displayed the results using pie chart.

	WN (7)	WSN (21)	MANET (28)
Problem 1	7	17	23
Problem 2	5	5	12
Problem 3	2	15	10
Problem 4	6	11	4
Problem 5	6	5	6
Problem 6	1	14	11
Problem 7	1	4	20
Problem 8	3	6	9

Table 11. References Identifying Key Management Problems

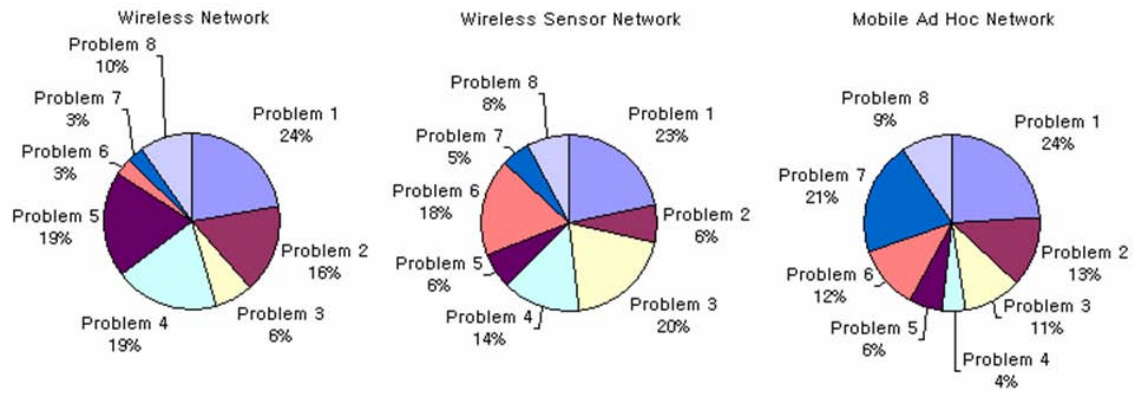

Figure 5. Percentage of Key Management References by Problem

4.3. Factors Affecting Key Management

4.3.1. Overview

In order to provide the critical factors of key management, twenty-eight references related to key management were used (See Appendix B). The critical factors of key management problems were identified and will be explained in the next section.

Additionally, we present the major factors in each secure wireless network from related fifty-six (See Appendix C).

4.3.2. Critical Factors of Key Management

Key management schemes are usually evaluated by the number of total keys the system must maintain, the number of keys each user receives, the size of public information, the time required to derive keys for access classes, and work needed to perform when the hierarchy or the set of users change (Atallah, 2005). The efficiency of a centralized key management scheme is primarily measured by re-key overhead at the key server that is defined as the average number of re-key messages transmitted by the key server to users per key updating, the re-key overhead at users that is defined as the average number of re-key messages received by the users per key updating, and storage overhead that is defined as the average number of keys stored at the key server and the users (Zhang, 2004).

A security domain is a collection of systems (servers, devices, and so on) that share a common set of keys and are attached to an administered network. Security domains provide a useful approach for dealing with logical keying structures for data protection in large-scale systems in which many objects must be protected (Michener, 2000).

Harris (2003) explains the three principles and six rules of key management. The principles are following: Key should not be in clear-text outside the cryptography device. All of key distribution and maintenance should be automated and hidden form the user. Backup copies should be available and easily accessible when required. In addition, the

rules are following: The key length should be long enough to provide the necessary level of protection. Keys should be stored and transmitted by secure means. The key's lifetime should correspond with the sensitivity of the data it is protecting. The more the key is used, the shorter its lifetime should be. Keys should be backed up or escrowed incase of emergencies. Keys should be properly destroyed when their lifetime comes to an end.

The most important design criteria for a key management system are listed below (Fumy, 1993).

1. Minimize the number and complexity of trusted mechanisms involved. Especially, minimize the involvement of central mechanisms.
2. Minimize physical activity, e.g., the use of couriers should be kept at a minimum (i.e., nonexistent if possible). This requirement also implies that for registration, entities should not have to travel far (for large systems, this suggests a hierarchical approach).
3. Minimize the need for physical security, e.g., the number and size of tamper-resistant devices, or the number of secure channels required.
4. Achieve maximum flexibility with regard to specific key distribution protocols and specific cryptographic algorithms.
5. Achieve maximum robustness (e.g., self-synchronization when keys are updated).
6. Ensure that if any one entity is dishonest, that entity may be exposed.

Table 12. Design Criteria for Key Management

4.3.3. Result and Analysis

The critical factors of key management that I identified are summarized in Table 13 below.

1. Key management is evaluated by the number of key, the information size, required time, needed work.
2. Security domains provide a useful approach for dealing with key management.
3. Key should not be in clear-text outside the cryptography device.
4. All of key distribution and maintenance should be automated and hidden form the user.
5. Backup copies should be available and easily accessible when required.
6. Minimize the number and complexity of trusted mechanisms and physical activity, and the need for physical security
7. Achieve maximum flexibility and robustness
8. Ensure that if one is dishonest, it may be exposed

Table 13. The Critical Factors of Key Management

There are many references that explain which key management philosophy is better in a particular network environment and how to manage key secrecy effectively. However, there are no abstract factors which seem to influence all wireless networks. Due to their unique characteristics, each network type is suitable for different environment. Wireless network (WNs) are used in the situation where there is infrastructure to support security. Wireless sensor networks (WSNs) are suitable for the

environment which does not require a lot of resources and computation capabilities. The network environments such as dynamic topology and no infrastructure make it possible to emerge the mobile ad hoc networks (MANETs). Table 14 and Figure 6 together summarize the fact that there are no dominating factors. Therefore, it is important to identify the characteristics of the network environment before considering a particular key management methodology.

Table 14 and Figure 6 show that there are no main dominating factors. Most factors influenced each of the secure wireless network. Moreover, these illustrate that some factors which affect the particular wireless network are not main factors in other wireless networks. Therefore, it is possible to solely suggest particular factors affecting general wireless network.

	WN (7)	WSN (21)	MANET (28)
Factor 1	7	20	24
Factor 2	6	17	14
Factor 3	1	18	14
Factor 4	4	3	22
Factor 5	3	12	17
Factor 6	4	7	6
Factor 7	5	15	6
Factor 8	3	17	3

Table 14. The Number of Key Management References Identifying Critical Factors

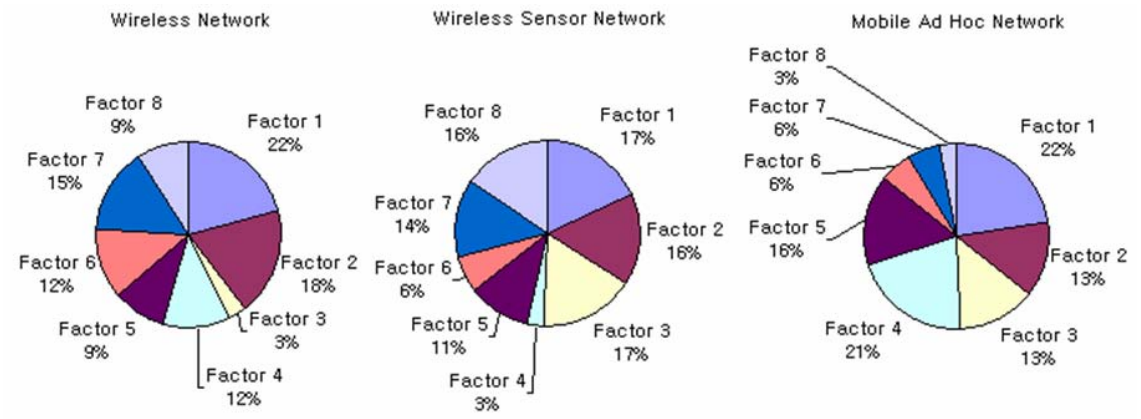

Figure 6. The Percentage of Key Management References Identifying Critical Factors

4.4. Key Management Solutions in Secured Networks

4.4.1. Overview

In this section, we will examine and discuss key management solutions in detail. Each key management solution will be explained and its strengths and weaknesses will be discussed. Finally, we will make suggestions which solution is suitable in each secure network environment.

4.4.2 Key Management Solutions

4.4.2.1. Partially Distributed Certificate Authority (PDCA)

Using a *(k, n)* threshold, Zhou (1999) proposed this solution in order to distribute the services of the certificate authority to specialized server nodes. Each of these nodes has a capability to generate a partial certificate using their share of the certificate signing key. However, a valid certificate can be obtained only by combining *k* such partial certificates.

The system contains three types of nodes; client, server and combiner nodes. The client nodes are the normal users of the network while the server and combiner nodes are part of the certificate authority. The server nodes are responsible for generating partial certificates and storing certificates in a directory structure allowing client nodes to request for the certificates of other nodes. The combiner nodes which are also server nodes are responsible for combining the partial certificates into a valid certificate. Although not stated implicitly by the authors the system also has an administrative authority which will be termed the dealer. The dealer is the only entity in the system that has knowledge of the complete certificate signing key sk_{CA}.

Every node in the network has a public/private key pair and it is the responsibility of the dealer to issue the initial certificate for the nodes public key as well as distributing the public key pk_{CA} of the certificate authority which is needed to verify the certificates.

The certificate authority as a whole has a public/private key pair, pk_{CA} / sk_{CA} of which the public key is known to all network nodes. The private key sk_{CA}, is shared among the server nodes according to Shamir's secret sharing scheme (Fokine, 2002).

Figure 7 illustrates the different components of the system.

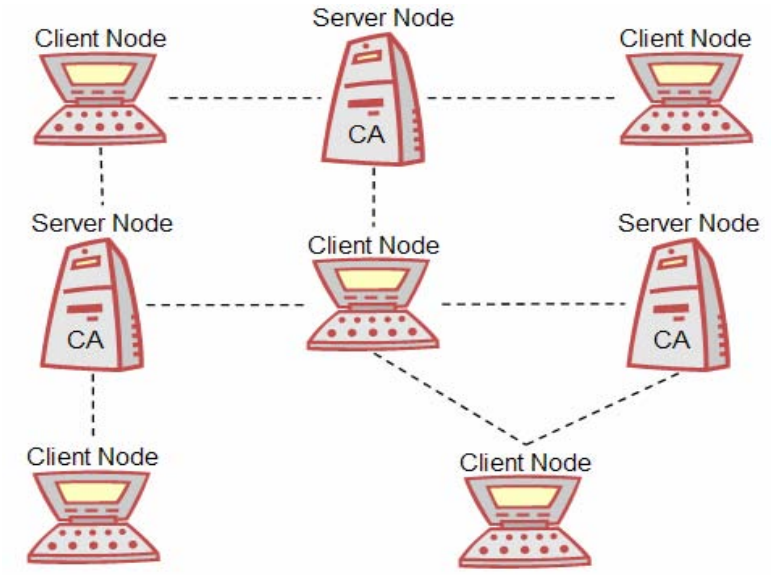

Figure 7. Partially Distributed Certificate Authority (Fokine, 2002)

4.4.2.2. Fully Distributed Certificate Authority (FDCA)

This solution is introduced by (Luo, 2000; Kong, 2001; Luo, 2002). In order to distribute an RSA certificate signing key to all nodes in the network, a *(k, n)* threshold scheme is used. It also uses verifiable and proactive secret sharing mechanisms to protect against denial of service attacks and compromise of the certificate signing key. The service of a certificate authority is distributed to a set of specialized server nodes. By using secret sharing, each of these nodes can generate partial certificates and by combining enough of them a valid certificate can be created.

In this solution, the capabilities of the CA are distributed to all nodes in the ad hoc network, see Figure 8. Any operations requiring the CA's private key sk_{CA} can only be performed by a coalition of k or more nodes. The services provided by the CA can be

grouped as certificate related services and system maintenance services. The certificate related services include certificate renewal and revocation.

The system maintenance services include incorporating joining nodes into the CA, i.e. provide them with their share of the CA's private key sk_{CA}. This service is called share initialization. The system maintenance also includes proactively updating the shares of the CA's private key to protect it from being compromised. This service is termed share update.

The availability of the service is based on the assumption that every node will have a minimum of k one-hop neighbors and that the nodes are provided with a valid certificate prior to their joining the network. The system then provides services to maintain and update these initial certificates (Fokine, 2002).

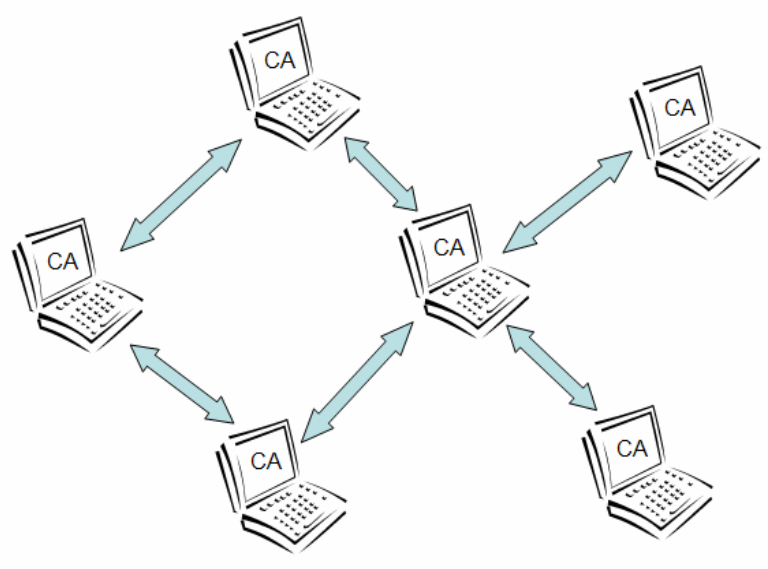

Figure 8. Fully Distributed Certificate Authority (Fokine, 2002)

4.4.2.3. Zero Knowledge Proofs (ZKP)

There are different possibilities of authentication, which use either a Trusted Third Part (TTP) or a Chain of Trust. Recently, a lot of research has been interested in the field of Zero Knowledge Proofs. In theory, Zero Knowledge Proofs (ZKPs) is introduced by (Goldwasser, 1991). This method provides a good solution to node identification. Zero Knowledge Proofs allow one party to prove its knowledge of a secret to another party without revealing any information of the secret itself.

Suppose that Alice knows a fact. She wants to convince Bob that she knows *P*, but she does not trust Bob. Thus, Alice does not want to reveal nay more knowledge to Bob than is necessary. What Alice needs is a zero-knowledge proof of *P*.

For example, suppose that Alice wants to prove to Bob that she really is Alice. Suppose for convenience that there is some authority that verifies identities. One possibility is that the authority could issue Alice identification. If this were contained on a device such as a smart card, Alice could simply show it to Bob. However, if Alice and Bob are communicating over a network, then Alice's identifying information would have to be transmitted to Bob over the network. On receiving it, Bob could use it to impersonate Alice. Even if Bob were trusted, an eavesdropper such as Alice's adversary Carol could do the same.

This situation also arises commonly in computer access control: Bob might then be a host computer or network server, and Alice's identification might be a password. If Alice uses her password to identify herself, her password is exposed to the host software as well as eavesdroppers; anyone who knows this password can impersonate Alice. It is thus desirable for Alice to be able to prove her identity without revealing any private

information. More generally, we need a scheme through which Alice can prove to Bob that she possesses something such as passwords without having to reveal it. Such a scheme is an example of a zero-knowledge proof. In fact, this example is the major practical use of zero-knowledge that has been suggested to date.

Here is one way that such a system could be organized. The authority decides on a number *N* used for everyone; for example, take $N = 77$. Everyone knows this number. The authority may then choose, for example, two numbers that form an ID for Alice. Suppose these are {58, 67}. Everyone knows Alice's ID. The authority then computes two other numbers {9, 10} that are given to Alice alone; she keeps these private. The latter numbers were chosen because $9^2 \times 58 \equiv 1 \pmod{77}$ and $10^2 \times 67 \equiv 1 \pmod{77}$. Now, Alice can identify herself to Bob by proving that she possesses the secret number {9, 10} without revealing them. Each time she wishes to do this, she can proceed as follows.

She can choose some random numbers such as {19, 24, 51} and compute

$$19^2 \equiv 53 \pmod{77}$$

$$24^2 \equiv 37 \pmod{77}$$

$$51^2 \equiv 60 \pmod{77}$$

Alice then sends {53, 37, 60} to Bob. Bob chooses a random 3 by 2 matrix of 0's and 1's, for example,

$$E = \begin{matrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{matrix}$$

Bob sends *E* to Alice. On receipt, Alice computes.

$$19 \times 9^0 \times 10^1 \equiv 36 \pmod{77}$$

$$24 \times 9^1 \times 10^0 \equiv 62 \pmod{77}$$

$$51 \times 9^1 \times 10^1 \equiv 47 \pmod{77}$$

Alice sends {36, 62, 47} to Bob. Finally, Bob can check to see that Alice is who she says she is. He does this by checking that

$$36^2 \times 58^0 \times 67^1 \equiv 53 \pmod{77}$$

$$62^2 \times 58^1 \times 67^0 \equiv 37 \pmod{77}$$

$$47^2 \times 58^1 \times 67^1 \equiv 60 \pmod{77}$$

The original numbers {53, 37, 60} that Alice sent reappear. Actually, this doesn't really prove Alice's identity; she could have been an impersonator. But the chances of an impersonator succeeding would have been only 1 in 64.

In an actual system, the number N would have been much larger (for example, 160 digits). Also, Alice would have been assigned an ID consisting of more number, for example, 4, by the authority, with a secret also consisting of four numbers. Furthermore, Alice would have generated more random numbers, for example, 5, to send to Bob. The ID numbers, secret numbers, and random numbers would have been about as large as *N*. This would have reduced an impersonator's chances of cheating successfully to about 1 in a million (more precisely 2^{-20}) if 4 and 5 are the parameters, which certainly would have convinced Bob of Alice's identity (Mollin, 2003).

4.4.2.4. Self Issued Certificates (SIC)

This solution is proposed by Hubaux (2001). This provides a public key management solution similar to Pretty Good Privacy (PGP) (Garfinkel, 1995) in the sense that certificates are issued by the users themselves without the aid of any certification authority.

This solution, like PGP, deals with the problem of distributing public keys in an authenticated manner. Unlike traditional PKI solutions, in PGP the public keys aren't certified by some trusted third party, e.g. a CA. Instead each user has the capability of certifying the public keys of other users. It is then up to each user to determine how much trust to place in a specific certificate. Figure 9 illustrates a simple example of how PGP works. Bob has issued a certificate to Chris thus stating that pk_{Chris} really is the public key belonging to Chris. Alice has also issued a certificate to Bob, indicating that pk_{Bob} is really the public key belonging to Bob. Alice also trusts Bob not to issue any false certificates, thus Alice will trust any certificates issued by him. Therefore having $cert_{Alice,Bob}$ and $cert_{Bob,Chris}$, Alice can verify that pk_{Chris} is authentic. She can then securely communicate with Chris even though they have never met (Fokine, 2002).

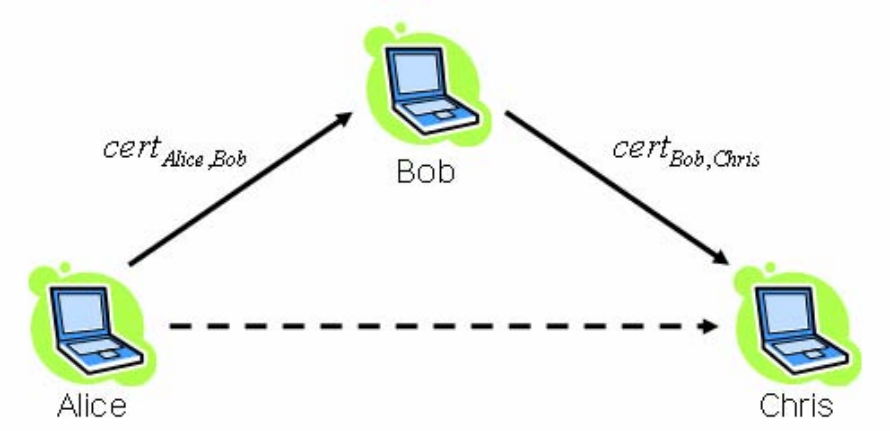

Figure 9. Example of a certificate chain (Fokine, 2002)

In PGP, public key servers, i.e. certificate directories are used to distribute certificates; however in ad hoc networks no such servers are available and therefore the solution proposed by Hubaux (2001) relies on the users to distribute and store the certificates themselves. Each user stores a small number of certificates that have been issued. When two users wish to authenticate each others' public keys, they try to find a certificate chain using only the certificates stored in their combined local certificate repositories (Fokine, 2002).

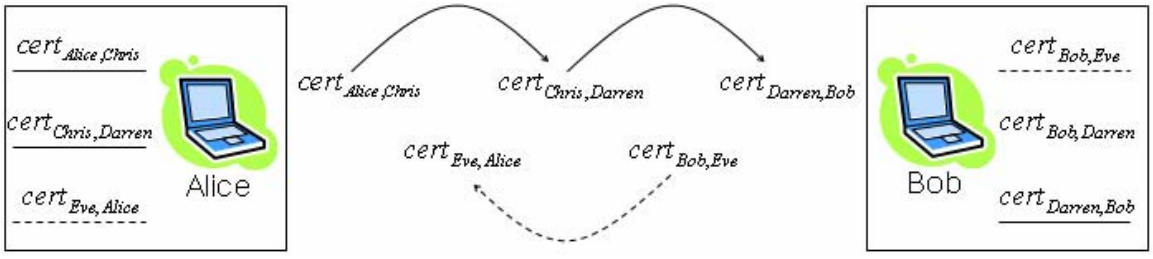

Figure 10. Building certificate chains (Fokine, 2002)

4.4.2.5. Password Authenticated Key Exchange (PAKE)

Asokan (2000) introduced a password authenticated group key agreement protocol. He considered a collaborative network scenario where a group of people wishes to establish a secure wireless network during a meeting. In order to obtain such a security, a written password is selected. The protocol used in this solution is based on the Diffie-Hellman key agreement protocol.

The meeting members have no means of authenticating the other members using e.g. digital certificates. Therefore a simple password is chosen and e.g. written on a whiteboard. Using this weak password the members can engage in the password authenticated Hypercube protocol which results in them sharing a strong secret. The key agreement protocol needs to be authenticated to protect against active attacks, e.g. man-in-the-middle attacks.

A number of group key establishment protocols are compared along with the Hypercube protocol. The nodes participating in the protocol are arranged as the vertices in a d-dimensional cube, a hypercube. The protocol then consists of d rounds of two-party Diffie-Hellman key exchange. During each round $j = 1, \ldots, d$ a node performs the two-party key exchange with its neighbor in the j:th dimension. In the first round each node i uses his own secret x_i as the exponent. In the following rounds the key obtained from the previous round is used as the secret exponent.

Figure 11 illustrates the Hypercube protocol where the number of participants is four, i.e. $d = 2$. In the first round nodes 1 and 2 perform a two-party Diffie-Hellman key exchange, in parallel nodes *3* and *4* do the same. After the first round the pairs *(1, 2)* and

(3, 4) share a common secret $k_{1,2}$ and $k_{3,4}$. In the second and final round nodes *1* and *3* perform a two-party Diffie-Hellman key exchange, as do nodes *2* and *4*. The key exchange in the previous round is now used as the secret exponent in the Diffie-Hellman key exchange. E.g. node *1* sends $g^{k_{1,2}} \bmod p$ to node *3* and node *3* sends $g^{k_{3,4}} \bmod p$ to node *1*. After the second round is complete all four nodes share a secret *k* (Fokine, 2002).

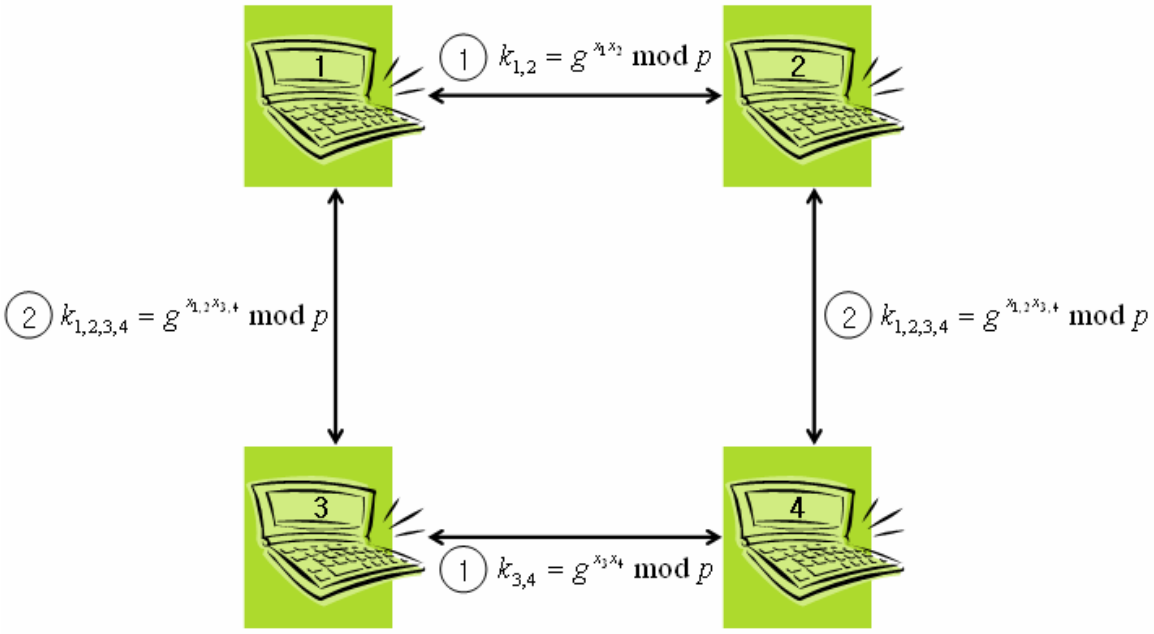

Figure 11. The Hypercube protocol used to provide four nodes (Fokine, 2002)

4.4.3. Analysis

Both Partially Distributed Certificate Authority (PDCA) and Fully Distributed Certificate Authority (FDCA) use the concept of *(k, n)* threshold in order to distribute the service of certificate authority. In PDCA, there are special server nodes which provide

generate partial certificates and allow client nodes to request for the certificates of other nodes. For this reason, it is required to select the special nodes. On the other hand, FDCA allows each node to certificate themselves without any special nodes. Strong certificates may be not expected depending on the function of each node. Zero Knowledge Proof (ZKP) allows identifying without revealing any information related secret. Although this requires less computation power, this may result in increasing overheads as increasing users. Self Issue Certificates (SIC) manage the key distribution in a similar fashion to Pretty Good Privacy (PGP). It does not require infrastructure, but the initial phase is required. Finally, Password Authenticated Key Exchange (PAKE) makes meeting members to share strong secret using weak password. However, it is group-oriented. The advantages and weaknesses are summarized in Table 15,

	Advantage	Weakness
PDCA	The solution is suitable for planned, long-term ad hoc networks. Since it is based on public key encryption it requires that the all the nodes are capable of performing the necessary computations.	This solution requires that a server- and organizational/administrative infrastructure is available and therefore is only applicable to a subset of ad hoc network applications.
FDCA	This solution is aimed towards planned, long-term ad hoc networks with nodes capable of public key encryption. However, since the service is distributed among all the nodes when they join the network, there is no need to elect or choose any specialized server nodes.	A larger number of shares are exposed to compromise since each node has its own share as compared to only the specialized server nodes in the partially distributed solution.
ZKP	ZKPs typically require significantly less computing power than traditional identification paradigms, which makes them especially appealing for ad hoc networks.	The problem with this proof is that it affords interaction between prover and verifier. It is means an increase of overheads in communication between the parties involved in the authentication process.
SIC	The main benefit of this solution is that it doesn't require any form of infrastructure neither routing, server or organizational/administrative.	It requires an initial phase during which its effectiveness is limited and therefore it is unsuitable for short-term networks.
PAKE	Using the weak password the members, they are able to share a strong secret.	This is a group-oriented solution since it doesn't allow for authentication of individual nodes.

Table 15. Advantages and Weaknesses of Solutions

From the advantages and weaknesses of each solution, we suggest which network is a suitable solutions. Table 16 illustrates the comparison in each wireless network. This table shows which solution may be more suitable for a given wireless network. PDCA and FDCA are suitable for WSNs and MANETs since the nodes in the network function as a router. ZKP is suitable for WNs and MANETs since it requires less computing power. SIC is suitable for WNs and MANETs. Since the initial phase is

required, many problems may occur in WSNs. PAKE have limitations using WSNs and MANETs where there is no infrastructure to support security services. Table 16 explains which solution is suitable to apply to each network environment.

	WN	WSN	MANET
PDCA		√	√
FDCA		√	√
ZKP		√	√
SIC	√		√
PAKE	√		

Table 16. A Comparison of Solutions in Each Wireless Network Environment

V. Discussion and Conclusions

5.1. Overview

In chapter 4, we examined the most important characteristics of implementing security in wireless network environments. We also identified critical factors which determine if a key management methodology is effective in a given network environment. We identified and discussed common problems encountered when deploying key management and discussed possible solutions. In this chapter, we will apply the knowledge we gained in chapter 4 and discuss them in the context of answering the research questions. Finally, we will present the findings of the research, the significance of research findings, and provide recommendations for future research.

5.2. Discussion

In chapter 1, we presented the primary research question and five related investigative questions in order to assess and identify existing key management techniques in secure communication network and to identify the strengths and weaknesses inherent in their design. The primary research question to be answered was *"What are characteristics in using Key Management in wireless network?"* and five investigated questions are below.

1) *What are the characteristics of various secure wireless communications?*
2) *What are the problems of implementing secure wireless network?*
3) *What are the critical success factors in deployment of a secure wireless network?*
4) *What cryptographic techniques are possible in secure wireless network?*

5) What is the advantages/weakness of each cryptography technique?

The first question is *what are the characteristics of various secure wireless communications?* In order to answer this question, we investigated the characteristics of various network environments. Generally, Wireless Networks (WN) have infrastructure to support security. The networks are easy and flexible to establish, but they are vulnerable to suffer from potential attack. Wireless Sensor Network (WSN) have unique characteristics such that low-power, self-power, and low cost. However, the sensor nodes have limited sources. Mobile ad hoc networks (MANETs) establish the temporary network without infrastructure. Due to this characteristic, this network is more flexible than wireless network, and has dynamic topology. However, this has critical problem of security.

The second question is *what are the problems of implementing secure wireless network?* The problems we identified in implementing secure network focused on the issues related to key management. The major problems identified are key distribution and the lack of resources such as storage and computational capability to enable encryption. In conventional networks, key distribution is centralized, uses fixed infrastructure, and is deployed by the organization to support the network. In contrast, the wireless network environment creates difficulties due to it lack of infrastructure. In addition, the nodes of wireless network typically have limited resources which severely limits the possible cryptographic solutions. Thus, if it is desired to implement strong security in a wireless network, the nodes in the network should be designed with sufficient storage and computational power to support the desired cryptography solution.

The third question is *what are the critical success factors in deployment of a secure wireless network?* In order to overcome the stated problems, we looked for critical issues when implementing key management. In order to secure a network, one must consider how key management is implemented. A review of the relevant literature, well defined policies, procedures, and processes to support key generation, key storage, key distribution, key updating, key revocation, and certificate service must be defined. In order to realize effective key management, it is important to identify the characteristics and problem of network environment and to employ appropriate solution in the network.

The fourth question is *what types of cryptography are used to secure wireless network?* This research identified several solutions used in securing network. The partially distributed certificate authority and fully distributed certificated authority employed the concept of *(k, n)* threshold. The zero knowledge proof is novel identity technique which proves its knowledge of a secret to another without revealing any information. Self issued certificate issues certificate without any aid of certification authority is similar to Pretty Good Privacy (PGP). Finally, password authenticated key exchange is authenticated group key agreement protocol using password.

The fifth question is *what is the advantages/weakness of each cryptography technique?* We examined the advantage and weakness of each solution. Partially distributed certificate authority and fully distributed certificate authority are designed to be suitable for ad hoc networks. Zero knowledge proof requires less computing power, but the network overhead is increased as the participants are increased. Self issued certificate does not require infrastructure. In order to effective communication, however,

an initial phase is preceded. In password authenticate key exchange, the member of a group are able to share a strong secret using the weak password.

5.3. Conclusion

The objective of research is to provide guidelines for successful implementation in secure wireless communication network. This research effort was an attempt to look for the critical factors in implementing key management in various wireless network environments in order to support secure communication in military operation.

In this research, we have found that secure communication must be supported by strong key management. In addition, when secure communications are constructed, the network environment should be identified and appropriate security methods should be provided. Even if a technically sound secure communications is constructed, the underlying security can be easily compromised without strong key management. It is recommended that WSN and MANET nodes be designed with increased computational and storage capability to support stronger cryptographic mechanisms.

5.4. Significance

The research finding have identified best practices and guidelines used when securing a wireless communications environment. A comparison between cryptographic solutions in terms of their strength and key management complexity was provided to enable the best selection for a given application. The research findings can aid in deploying secure communications in the military operations, law enforcement, and disaster response domains.

5.5. Future Research

This research focused only on the wireless network environment. A broader study which examines all network topologies would provide additional insight into problems and solutions in key management.

Future research could explore the military communication environment in detail and possible compare and contrast with the non-military communication environment. This would prove beneficial because of the unique characteristics of military communication could be identified and the possible solutions could be suggested. This work could provide a similar analysis to this study with the intent of providing effective guidelines to implement securing military communication network.

5.6. Summary

Key management issues are very important in secure communications network. Since existing key management solutions are based on fixed networks, advanced wireless network technologies such as wireless sensor network and mobile ad hoc network require more interests and effort to apply to military network. In this chapter, we answered the research questions we formulated and identified important guidelines when constructing a secure wireless networks.

APPENDIX A: Literatures of Wireless Network Environment [56]

Wireless Networks (WNs) [23]

Ahmad, A., Rizvi, M. E., & Olariu, S. (2005). Common data security network (CDSN). *Q2SWinet '05: Proceedings of the 1st ACM international workshop on quality of service \& security in wireless and mobile networks*, Montreal, Quebec, Canada, 1-7. from http://doi.acm.org/10.1145/1089761.1089763

Allen, J., & Wilson, J. (2002). Securing a wireless network. *SIGUCCS '02: Proceedings of the 30th annual ACM SIGUCCS conference on user services*, Providence, Rhode Island, USA, 213-215. from http://doi.acm.org/10.1145/588646.588696

Arbaugh, W. A. (2003). Wireless security is different. *Computer, 36*(8), 99-101.

Arbaugh, W. A., Shankar, N., Wan, Y. C. J., & Kan Zhang. (2002). Your 80211 wireless network has no clothes. *Wireless Communications, IEEE [See also IEEE Personal Communications], 9*(6), 44-51.

Bhagyavati, Summers, W. C., & DeJoie, A. (2004). Wireless security techniques: An overview. *InfoSecCD '04: Proceedings of the 1st annual conference on information security curriculum development*, Kennesaw, Georgia, 82-87. from http://doi.acm.org/10.1145/1059524.1059541

Bharghavan, V. (1994). Secure wireless LANs. *CCS '94: Proceedings of the 2nd ACM conference on computer and communications security*, Fairfax, Virginia, United States, 10-17. from http://doi.acm.org/10.1145/191177.191181

Chen, J., Jiang, M., & Liu, Y. (2005). Wireless LAN security and IEEE 802.11i. *Wireless Communications, IEEE [See also IEEE Personal Communications], 12*(1), 27-36.

Eisinger, J., Winterer, P., & Becker, B. (2005). Securing wireless networks in a university environment. 312-316.

Godber, A., & Dasgupta, P. (2002). Secure wireless gateway. *WiSE '02: Proceedings of the 3rd ACM workshop on wireless security*, Atlanta, GA, USA, 41-46. from http://doi.acm.org/10.1145/570681.570686

Housley, R., & Arbaugh, W. (2003). Security problems in 802.11-based networks. *Communications of the ACM, 46*(5), 31-34.

Karnik, A., & Passerini, K. (2005). Wireless network security - a discussion from a business perspective. 261-267.

Olariu, S., Eltoweissy, M., & Younis, M. (2005). ANSWER: Autonomous wireless sensor network. *Q2SWinet '05: Proceedings of the 1st ACM international workshop on quality of service \& security in wireless and mobile networks*, Montreal, Quebec, Canada, 88-95. from http://doi.acm.org/10.1145/1089761.1089776

Park, S. H., Ganz, A., & Ganz, Z. (1998). Security protocol for IEEE 802.11 wireless local area network. *Mob.Netw.Appl., 3*(3), 237-246.

Patiyoot, D., & Shepherd, S. J. (1998). Security issues for wireless ATM networks. *3* 1555-1559 vol.3.

Patiyoot, D., & Shepherd, S. J. (1999). Cryptographic security techniques for wireless networks. *SIGOPS Oper.Syst.Rev., 33*(2), 36-50.

Potter, B. (2003). Wireless security's future. *Security & Privacy Magazine, IEEE, 1*(4), 68-72.

Russell, S. F. (2001). Wireless network security for users. 172-177.

Schmidt, T., & Townsend, A. (2003). Why wi-fi wants to be free. *Communications of the ACM, 46*(5), 47-52.

Shin, M., Ma, J., Mishra, A., & Arbaugh, W. A. (2006). Wireless network security and interworking. *Proceedings of the IEEE, 94*(2), 455-466.

Soliman, H. S., & Omari, M. (2005). Application of synchronous dynamic encryption system in mobile wireless domains. *Q2SWinet '05: Proceedings of the 1st ACM international workshop on quality of service \& security in wireless and mobile networks*, Montreal, Quebec, Canada, 24-30. from http://doi.acm.org/10.1145/1089761.1089766

Tonesi, D., & Salgarelli, L. (2005). Smart PSK provisioning: A key-management and authentication scheme for wireless LANs. 119-124.

Yang, H., Ricciato, F., Lu, S., & Zhang, L. (2006). Securing a wireless world. *Proceedings of the IEEE, 94*(2), 442-454.

Zahur, Y., & Yang, T. A. (2004). Wireless LAN security and laboratory designs. *J.Comput.Small Coll., 19*(3), 44-60.

Wireless Sensor Netowork (WSNs) [18]

Bai, H., Atiquzzaman, M., & Lilja, D. (2004). Wireless sensor network for aircraft health monitoring. 748-750.

Bilstrup, U., Sjoberg, K., Svensson, B., & Wiberg, P. -. (2003). Capacity limitations in wireless sensor networks. *1* 529-536 vol.1.

Brownfield, M., Yatharth Gupta, & Davis, N. (2005). Wireless sensor network denial of sleep attack. 356-364.

Choi, S., Kim, B., Park, J., Kang, C., & Eom, D. (2004). An implementation of wireless sensor network. *Consumer Electronics, IEEE Transactions on, 50*(1), 236-244.

Culler, D. E., & Hong, W. (2004). Introduction. *Communications of the ACM, 47*(6), 30-33.

Dai, S., Jing, X., & Li, L. (2005). Research and analysis on routing protocols for wireless sensor networks. *1* 407-411 Vol. 1.

Hu, F., Sheony, N., & Liu, X. (2005). Robust security in large-scale wireless actuator and sensor networks: A low energy two-level implementation. 850-854.

Hu, F., & Cao, X. (2005). Security in wireless actor & sensor networks (WASN): Towards a hierarchical re-keying design. *2* 528-533 Vol. 2.

Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: A link layer security architecture for wireless sensor networks. *SenSys '04: Proceedings of the 2nd international conference on embedded networked sensor systems*, Baltimore, MD, USA, 162-175. from http://doi.acm.org/10.1145/1031495.1031515

Nadeem, T., & Ashok Agrawala. (2005). Performance of IEEE 802.11 based wireless sensor networks in noisy environments. 471-476.

Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM, 47*(6), 53-57.

Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wirel.Netw.*, *8*(5), 521-534.

Pietro, R. D., Mancini, L. V., & Mei, A. (2003). Random key-assignment for secure wireless sensor networks. *SASN '03: Proceedings of the 1st ACM workshop on security of ad hoc and sensor networks*, Fairfax, Virginia, 62-71. from http://doi.acm.org/10.1145/986858.986868

Pottie, G. J., & Kaiser, W. J. (2000). Wireless integrated network sensors. *Communications of the ACM, 43*(5), 51-58.

Rajaravivarma, V., Yi Yang, & Teng Yang. (2003). An overview of wireless sensor network and applications. 432-436.

Romer, K., & Mattern, F. (2004). The design space of wireless sensor networks. *Wireless Communications, IEEE [See also IEEE Personal Communications], 11*(6), 54-61.

Tie, L., & Li, J. (2005). Combinatorial optimization for wireless sensor networks. 439-442.

Ulema, M. (2004). Wireless sensor networks: Architectures, protocols, and management. *1* 931 Vol.1.

Mobile Ad Hoc Network (MANETs) [15]

Aboudagga, N., Refaei, M. T., Eltoweissy, M., DaSilva, L. A., & Quisquater, J. (2005). Authentication protocols for ad hoc networks: Taxonomy and research issues. *Q2SWinet '05: Proceedings of the 1st ACM international workshop on quality of service \& security in wireless and mobile networks*, Montreal, Quebec, Canada, 96-104. from http://doi.acm.org/10.1145/1089761.1089777

Alampalayam, S., Kumar, A., & Srinivasan, S. (2005). Mobile ad hoc network security - a taxonomy. *2* 839-844.

Bouam, S., & Ben-Othman, J. (2003). Data security in ad hoc networks using multipath routing. *2* 1331-1335 vol.2.

Buttyan, L., & Hubaux, J. (2003). Report on a working session on security in wireless ad hoc networks. *SIGMOBILE Mob.Comput.Commun.Rev.*, *7*(1), 74-94.

Capkun, S., Hubaux, J., & Buttyan, L. (2003). Mobility helps security in ad hoc networks. *MobiHoc '03: Proceedings of the 4th ACM international symposium on mobile ad hoc networking \& computing*, Annapolis, Maryland, USA, 46-56. from http://doi.acm.org/10.1145/778415.778422

Hu, Y., Perrig, A., & Johnson, D. B. (2002). Ariadne:: A secure on-demand routing protocol for ad hoc networks. *MobiCom '02: Proceedings of the 8th annual international conference on mobile computing and networking*, Atlanta, Georgia, USA, 12-23. from http://doi.acm.org/10.1145/570645.570648

Jiang, T., & Li, Q. (2004). A secure routing protocol for mobile ad-hoc networks. *5* 2825-2829 vol.5.

Keoh, S. L., & Lupu, E. (2002). Towards flexible credential verification in mobile ad-hoc networks. *POMC '02: Proceedings of the second ACM international workshop on principles of mobile computing*, Toulouse, France, 58-65. from http://doi.acm.org/10.1145/584490.584503

Li, S., & Wang, X. (2004). Ad hoc network security with geographical aids. *1* 474-479 Vol.1.

Manikopoulos, C., & Li Ling. (2003). Architecture of the mobile ad-hoc network security (MANS) system. *4* 3122-3127 vol.4.

Messerges, T. S., Cukier, J., Kevenaar, T. A. M., Puhl, L., Struik, R., & Callaway, E. (2003). A security design for a general purpose, self-organizing, multihop ad hoc wireless network. *SASN '03: Proceedings of the 1st ACM workshop on security of ad hoc and sensor networks*, Fairfax, Virginia, 1-11. from http://doi.acm.org/10.1145/986858.986860

Suen, T., & Yasinsac, A. (2005). Ad hoc network security: Peer identification and authentication using signal properties. 432-433.

Xie, B., & Kumar, A. (2004). A framework for integrated internet and ad hoc network security. *1* 318-324 Vol.1.

Yang, H., Meng, X., & Lu, S. (2002). Self-organized network-layer security in mobile ad hoc networks. *WiSE '02: Proceedings of the 3rd ACM workshop on wireless security*, Atlanta, GA, USA, 11-20. from http://doi.acm.org/10.1145/570681.570683

Yi, P., Yao, Y., Hou, Y., Zhong, Y., & Zhang, S. (2004). Securing ad hoc networks through mobile agent. *InfoSecu '04: Proceedings of the 3rd international conference on information security*, Shanghai, China, 125-129. from http://doi.acm.org/10.1145/1046290.1046315

APPENDIX B: Literatures of Key Management [28]

IEEE Standards for Local and Metropolitan Area Networks: Supplement to Standard for Interoperable LAN/MAN Security (SILS) - Key Management (Clause 3)(1998).

Abdalla, M., Shavitt, Y., & Wool, A. (2000). Key management for restricted multicast using broadcast encryption. *IEEE/ACM Trans.Netw., 8*(4), 443-454.

Adamouski, F. J. (1998). Encryption technology other than PKI. 108-116.

Atallah, M. J., Frikken, K. B., & Blanton, M. (2005). Dynamic and efficient key management for access hierarchies. *CCS '05: Proceedings of the 12th ACM conference on computer and communications security*, Alexandria, VA, USA, 190-202. from http://doi.acm.org/10.1145/1102120.1102147

Branstad, D. K., & Balenson, D. M. (2000). Policy-based cryptographic key management: Experience with the KRP project. *1* 103-114 vol.1.

Comba, P. G. (1986). Approaches to cryptographic key management. *PCS '86: Proceedings of the northeast ACM symposium on personal computer security*, Waltham, Massachusetts, United States, 38-45. from http://doi.acm.org/10.1145/318772.318781

Das, M. L., Saxena, A., Gulati, V. P., & Phatak, D. B. (2005). Hierarchical key management scheme using polynomial interpolation. *SIGOPS Oper.Syst.Rev., 39*(1), 40-47.

Fumy, W., & Landrock, P. (1993). Principles of key management. *Selected Areas in Communications, IEEE Journal on, 11*(5), 785-793.

Ghosh, A., & Anjum, F. (2005). Last hop topology sensitive multicasting key managment. *Q2SWinet '05: Proceedings of the 1st ACM international workshop on quality of service \& security in wireless and mobile networks*, Montreal, Quebec, Canada, 63-70. from http://doi.acm.org/10.1145/1089761.1089773

Gutmann, P. (2004). Simplifying public key management. *Computer, 37*(2), 101-103.

Harn, L., & Hung-Yu Lin. (1993). Key management for decentralized computer network services. *Communications, IEEE Transactions on, 41*(12), 1777-1779.

He Ge. (2005). An efficient key management scheme for pervasive computing. 657-661.

Jansen, W. A. (1993). A second look at the SDNS key management protocol. 74-81.

Lin, C., Lee, W., & Ho, Y. (2005). An efficient hierarchical key management scheme using symmetric encryptions. *2* 399-402 vol.2.

Michener, J. R., & Acar, T. (2000). Security domains: Key management in large-scale systems. *Software, IEEE, 17*(5), 52-58.

Neumann, P. G. (1997). Crypto key management. *Communications of the ACM, 40*(8), 136.

Park, C., & Lee, D. (2001). Secure and efficient key management for dynamic multicast groups. *SIGOPS Oper.Syst.Rev., 35*(4), 32-38.

Park, J. S., Chandramohan, P., Zak, A., & Giordano, J. (2004). Fine-grained, scalable, and secure key management scheme for trusted military message systems. *MILCOM 2004 - 2004 IEEE military communications conference, oct 31-nov 3 2004, 3* 1652-1658.

Pinkas, B. (2004). Efficient state updates for key management. *Proceedings of the IEEE, 92*(6), 910-917.

Rafaeli, S., & Hutchison, D. (2003). A survey of key management for secure group communication. *ACM Comput.Surv., 35*(3), 309-329.

Reiter, M. K., Franklin, M. K., Lacy, J. B., & Wright, R. N. (1996). The \Ω key management service. *CCS '96: Proceedings of the 3rd ACM conference on computer and communications security*, New Delhi, India, 38-47. from http://doi.acm.org/10.1145/238168.238184

Samarati, P., Reiter, M. K., & Jajodia, S. (2001). An authorization model for a public key management service. *ACM Trans.Inf.Syst.Secur., 4*(4), 453-482.

Tseng, Y. (2003). A scalable key-management scheme with minimizing key storage for secure group communications. *Int.J.Netw.Manag., 13*(6), 419-425.

Witzke, E. L., & Pierson, L. G. (1994). Key management for large scale end-to-end encryption. 76-79.

Wool, A. (2000). Key management for encrypted broadcast. *ACM Trans.Inf.Syst.Secur., 3*(2), 107-134.

Yang, C., Li, C., & Cheung, R. (2004). Cryptographic key management solution in a role hierarchy. *1* 575-578 Vol.1.

Zhang, Q., & Wang, Y. (2004). A centralized key management scheme for hierarchical access control. *4* 2067-2071 Vol.4.

Zhu Yujun, Wang Bai, & Chen Junliang. (1998). Secret key management based on variable authentication code in UPT system. 5 pp. vol.1.

APPENDIX C: Literatures of KM in Wireless Network [56]

Key Management in Wireless Networks (WNs) [7]

Di Pietro, R., Mancini, L. V., & Jajodia, S. (2002). Efficient and secure keys management for wireless mobile communications. *Proceedings of the second international workshop on principles of mobile commerce POMC '2002, oct 30-31 2002*, 66-73. from http://dx.doi.org/10.1145/584490.584504

Gu, Q., Liu, P., Lee, W. -., & Chu, C. -. (2005). KTR: An efficient key management scheme for air access control. 499-501.

Kostas, T., Kiwior, D., Rajappan, G., & Dalal, M. (2003). Key management for secure multicast group communication in mobile networks. *2* 41-43 vol.2.

Labiod, H., & Duffau, R. (2004). KMS: A key management system for multi-provider interconnected wi-fi WLANs. *4* 2061-2066 Vol.4.

Yan Sun, Trappe, W., & Liu, K. J. R. (2004). A scalable multicast key management scheme for heterogeneous wireless networks. *Networking, IEEE/ACM Transactions on, 12*(4), 653-666.

Yan Sun, Trappe, W., & Liu, K. J. R. (2002). An efficient key management scheme for secure wireless multicast. *2* 1236-1240 vol.2.

Yan Sun, Trappe, W., & Ray Liu, K. J. (2003). Topology-aware key management schemes for wireless multicast. *IEEE global telecommunications conference GLOBECOM'03, dec 1-5 2003, 3* 1471-1475. from http://dx.doi.org/10.1109/GLOCOM.2003.1258482

Key Management in Wireless Sensor Netowork (WSNs) [21]

Chan, S., Poovendran, R., & Sun, M. (2005). A key management scheme in distributed sensor networks using attack probabilities. *2* 1007-1011.

Chen, X., & Drissi, J. (2005). An efficient key management scheme in hierarchical sensor networks. 841-846.

Chorzempa, M., Park, J. -., & Eltoweissy, M. (2005). SECK: Survivable and efficient clustered keying for wireless sensor networks. 453-458.

Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J., & Khalili, A. (2005). A pairwise key predistribution scheme for wireless sensor networks. *ACM Trans.Inf.Syst.Secur., 8*(2), 228-258.

Du, W., Wang, R., & Ning, P. (2005). An efficient scheme for authenticating public keys in sensor networks. *MobiHoc '05: Proceedings of the 6th ACM international symposium on mobile ad hoc networking and computing*, Urbana-Champaign, IL, USA, 58-67. from http://doi.acm.org/10.1145/1062689.1062698

Eltoweissy, M., Younis, M., & Ghumman, K. (2004). Lightweight key management for wireless sensor networks. 813-818.

Huang, D., Mehta, M., Medhi, D., & Harn, L. (2004). Location-aware key management scheme for wireless sensor networks. *SASN '04: Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks*, Washington DC, USA, 29-42. from http://doi.acm.org/10.1145/1029102.1029110

Ito, T., Ohta, H., Matsuda, N., & Yoneda, T. (2005). A key pre-distribution scheme for secure sensor networks using probability density function of node deployment. *SASN '05: Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks*, Alexandria, VA, USA, 69-75. from http://doi.acm.org/10.1145/1102219.1102233

Jolly, G., Kuscu, M. C., Kokate, P., & Younis, M. (2003). A low-energy key management protocol for wireless sensor networks. 335-340 vol.1.

Lai, B. C., Hwang, D. D., Kim, S. P., & Verbauwhede, I. (2004). Reducing radio energy consumption of key management protocols for wireless sensor networks. *ISLPED '04: Proceedings of the 2004 international symposium on low power electronics and design*, Newport Beach, California, USA, 351-356. from http://doi.acm.org/10.1145/1013235.1013320

Liu, D., & Ning, P. (2003). Location-based pairwise key establishments for static sensor networks. *SASN '03: Proceedings of the 1st ACM workshop on security of ad hoc and sensor networks*, Fairfax, Virginia, 72-82. from http://doi.acm.org/10.1145/986858.986869

Liu, D., Ning, P., & Du, W. (2005). Group-based key pre-distribution in wireless sensor networks. *WiSe '05: Proceedings of the 4th ACM workshop on wireless security*, Cologne, Germany, 11-20. from http://doi.acm.org/10.1145/1080793.1080798

Park, J., Kim, Z., & Kim, K. (2005). State-based key management scheme for wireless sensor networks. 819-825.

Pietro, R. D., Mancini, L. V., & Mei, A. (2003). Random key-assignment for secure wireless sensor networks. *SASN '03: Proceedings of the 1st ACM workshop on security of ad hoc and sensor networks*, Fairfax, Virginia, 62-71. from http://doi.acm.org/10.1145/986858.986868

Price, A., Kosaka, K., & Chatterjee, S. (2005). A key pre-distribution scheme for wireless sensor networks. 253-260.

RuiYing Du, HuiJuan Tu, & Wen Song. (2005). An efficient key management scheme for secure sensor networks. 279-283.

Wadaa, A., Olariu, S., & Wilson, L. (2004). Scalable cryptographic key management in wireless sensor networks. 796-802.

Wang, L., Chen, Z., & Jiang, X. (2005). Researches on scheme of pairwise key establishment for distributed sensor networks. *WMuNeP '05: Proceedings of the 1st ACM workshop on wireless multimedia networking and performance modeling*, Montreal, Quebec, Canada, 54-61. from http://doi.acm.org/10.1145/1089737.1089747

Wenliang Du, Jing Deng, Han, Y. S., Shigang Chen, & Varshney, P. K. (2004). A key management scheme for wireless sensor networks using deployment knowledge. *1* 597.

Zhen Yu, & Yong Guan. (2005). A robust group-based key management scheme for wireless sensor networks. *4* 1915-1920 Vol. 4.

Zhou, L., Ni, J., & Ravishankar, C. V. (2005). Efficient key establishment for group-based wireless sensor deployments. *WiSe '05: Proceedings of the 4th ACM workshop on wireless security*, Cologne, Germany, 1-10. from http://doi.acm.org/10.1145/1080793.1080797

Key Management in Mobile Ad Hoc Network (MANETs) [28]

Balachandran, R. K., Ramamurthy, B., Xukai Zou, & Vinodchandran, N. V. (2005). CRTDH: An efficient key agreement scheme for secure group communications in wireless ad hoc networks. *2* 1123-1127 Vol. 2.

Balasubramanian, A., Mishra, S., & Sridhar, R. (2005). Analysis of a hybrid key management solution for ad hoc networks. *4* 2082-2087 Vol. 4.

Bing Wu, Jie Wu, Fernandez, E. B., & Magliveras, S. (2005). Secure and efficient key management in mobile ad hoc networks. 288a-288a.

Budakoglu, C., & Gulliver, T. A. (2004). Hierarchical key management for mobile ad-hoc networks. *4* 2735-2738 Vol. 4.

Capkun, S., Buttyan, L., & Hubaux, J. -. (2003). Self-organized public-key management for mobile ad hoc networks. *Mobile Computing, IEEE Transactions on, 2*(1), 52-64.

Chan, A. C. -. (2004). Distributed symmetric key management for mobile ad hoc networks. *4* 2414-2424 vol.4.

Erdem, O. M. (2004). EDKM: Efficient distributed key management for mobile ad hoc networks. *1* 325-330 Vol.1.

Erdem, O. M. (2004). Efficient self-organized key management for mobile ad hoc networks. *4* 2185-2190 Vol.4.

Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. *Proceedings of the 9th ACM conference on computer and communications security, nov 18-22 2002*, 41-47. from http://dx.doi.org/10.1145/586110.586117

Gang Xu, & Iftode, L. (2004). Locality driven key management architecture for mobile ad-hoc networks. 436-446.

Hadjichristofi, G. C., Adams, W. J., & Davis, N. J., IV. (2005). A framework for key management in mobile ad hoc networks. *2* 568-573 Vol. 2.

Hongmei Deng, Mukherjee, A., & Agrawal, D. P. (2004). Threshold and identity-based key management and authentication for wireless ad hoc networks. *1* 107-111 Vol.1.

Kitada, Y., Watanabe, A., Sasase, I., & Takemori, K. (2005). On demand distributed public key management for wireless ad hoc networks. 454-457.

Lehane, B., Dolye, L., & O'Mahony, D. (2005). Ad hoc key management infrastructure. *2* 540-545 Vol. 2.

Lehane, B., Doyle, L., & O'Mahony, D. (2003). Shared RSA key generation in a mobile ad hoc network. *2* 814-819 Vol.2.

Li, R., Li, J., Kameda, H., & Liu, P. (2004). Localized public-key management for mobile ad hoc networks. *2* 1284-1289 Vol.2.

Li, X., Wang, Y., & Frieder, O. (2002). Efficient hybrid key agreement protocol for wireless ad hoc networks. 404-409.

Merwe, J. v. d., Dawoud, D., & McDonald, S. (2005). Fully self-organized peer-to-peer key management for mobile ad hoc networks. *WiSe '05: Proceedings of the 4th ACM workshop on wireless security*, Cologne, Germany, 21-30. from http://doi.acm.org/10.1145/1080793.1080799

Moharrum, M., Mukkamala, R., & Eltoweissy, M. (2004). TKGS: Verifiable threshold-based key generation scheme in open wireless ad hoc networks. 31-36.

Ramkumar, M., & Memon, N. (2005). An efficient key predistribution scheme for ad hoc network security. *Selected Areas in Communications, IEEE Journal on, 23*(3), 611-621.

Raya, M., & Hubaux, J. (2005). The security of vehicular ad hoc networks. *SASN '05: Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks*, Alexandria, VA, USA, 11-21. from http://doi.acm.org/10.1145/1102219.1102223

Seys, S., & Preneel, B. (2005). The wandering nodes: Key management for low-power mobile ad hoc networks. 916-922.

Wuxu Peng, Yalin Wang, & Makki, K. (2004). Dynamic key management for secure routing in LCMRMG MANET. 227-232.

Xu, S. (2005). On the security of group communication schemes based on symmetric key cryptosystems. *SASN '05: Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks*, Alexandria, VA, USA, 22-31. from http://doi.acm.org/10.1145/1102219.1102224

Yi, S., & Kravets, R. (2004). Composite key management for ad hoc networks. 52-61.

Yi, S., & Kravets, R. (2002). Key management for heterogeneous ad hoc wireless networks. 202-203.

Younis, M., Ghumman, K., & Eltoweissy, M. (2005). Key management in wireless ad hoc networks: Collusion analysis and prevention. *24th IEEE international performance, computing, and communications conference, IPCCC 2005, apr 7-9 2005*, 199-203.

Zhang, Y., Liu, W., Lou, W., Fang, Y., & Kwon, Y. (2005). AC-PKI: Anonymous and certificateless public-key infrastructure for mobile ad hoc networks.

Bibliography

Aboudagga, N., Refaei, M. T., Eltoweissy, M., DaSilva, L. A., & Quisquater, J. (2005). Authentication protocols for ad hoc networks: Taxonomy and research issues. *Q2SWinet '05: Proceedings of the 1st ACM international workshop on quality of service \& security in wireless and mobile networks*, Montreal, Quebec, Canada, 96-104. from http://doi.acm.org/10.1145/1089761.1089777

Alampalayam, S., Kumar, A., & Srinivasan, S. (2005). Mobile ad hoc network security - a taxonomy. *2* 839-844.

Allen, J., & Wilson, J. (2002). Securing a wireless network. *SIGUCCS '02: Proceedings of the 30th annual ACM SIGUCCS conference on user services*, Providence, Rhode Island, USA, 213-215. from http://doi.acm.org/10.1145/588646.588696

Arbaugh, W. A. (2003). Wireless security is different. *Computer, 36*(8), 99-101.

Asokan, N., & Ginzboorg, P. (2000). Key agreement in ad hoc networks. *Computer Communications, 23*(17), 1627-1637.

Atallah, M. J., Frikken, K. B., & Blanton, M. (2005). Dynamic and efficient key management for access hierarchies. *CCS '05: Proceedings of the 12th ACM conference on computer and communications security*, Alexandria, VA, USA, 190-202. from http://doi.acm.org/10.1145/1102120.1102147

Avoine, G., & Vaudenay, S. (2002). Cryptography with guardian angels: Bringing civilization to pirates. *ACM Mobile Computing and Communications Review (MC2R), 6*(4)

Awerbuch, B., Holmer, D., Nita-Rotaru, C., & Rubens, H. (2002). An on-demand secure routing protocol resilient to byzantine failures. *WiSE '02: Proceedings of the 3rd ACM workshop on wireless security*, Atlanta, GA, USA, 21-30. from http://doi.acm.org/10.1145/570681.570684

Bai, H., Atiquzzaman, M., & Lilja, D. (2004). Wireless sensor network for aircraft health monitoring. 748-750.

Bakirdan, A., Qaddour, J., & Jalozie, I. K. (2003). Security algorithms in wireless LAN: Proprietary or nonproprietary. *3* 1425-1429 vol.3.

Bechler, M., Hof, H. -., Kraft, D., Pahlke, F., & Wolf, L. (2004). A cluster-based security architecture for ad hoc networks. *4* 2393-2403 vol.4.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly, 11*(3), 369-388.

Bharghavan, V. (1994). Secure wireless LANs. *CCS '94: Proceedings of the 2nd ACM conference on computer and communications security*, Fairfax, Virginia, United States, 10-17. from http://doi.acm.org/10.1145/191177.191181

Bilstrup, U., Sjoberg, K., Svensson, B., & Wiberg, P. -. (2003). Capacity limitations in wireless sensor networks. *1* 529-536 vol.1.

Bing Wu, Jie Wu, Fernandez, E. B., & Magliveras, S. (2005). Secure and efficient key management in mobile ad hoc networks. 288a-288a.

Binkley, J., & Trost, W. (2001). Authenticated ad hoc routing at the link layer for mobile systems. *Wirel.Netw., 7*(2), 139-145.

Bouam, S., & Ben-Othman, J. (2003). Data security in ad hoc networks using multipath routing. *2* 1331-1335 vol.2.

Brownfield, M., Yatharth Gupta, & Davis, N. (2005). Wireless sensor network denial of sleep attack. 356-364.

Buchegger, S., & and Boudec, J. (2002). Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in distributed ad-hoc networks. *MobiHoc,*

Budakoglu, C., & Gulliver, T. A. (2004). Hierarchical key management for mobile ad-hoc networks. *4* 2735-2738 Vol. 4.

Buttyan, L., & Hubaux, J. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications, 8*(5), 579-592.

Capkun, S., Buttyan, L., & Hubaux, J. -. (2003). Self-organized public-key management for mobile ad hoc networks. *Mobile Computing, IEEE Transactions on, 2*(1), 52-64.

Chen, J., Jiang, M., & Liu, Y. (2005). Wireless LAN security and IEEE 802.11i. *Wireless Communications, IEEE [See also IEEE Personal Communications], 12*(1), 27-36.

Chen, X., & Drissi, J. (2005). An efficient key management scheme in hierarchical sensor networks. 841-846.

Choi, S., Kim, B., Park, J., Kang, C., & Eom, D. (2004). An implementation of wireless sensor network. *Consumer Electronics, IEEE Transactions on, 50*(1), 236-244.

Creswell, J. W. (2003). *Research design : Qualitative & quantitative approaches* (2nd ed.). Thousand Oaks: Sage Publications.

Dai, S., Jing, X., & Li, L. (2005). Research and analysis on routing protocols for wireless sensor networks. *1* 407-411 Vol. 1.

Dam, K. W. (1996). *Cryptography's role in securing the information society*. Washington, D.C.: National Academy Press.

Dankers, J., Garefalakis, T., Schaffelhofer, R., & Wright, T. (2002). Public key infrastructure in mobile systems. *Electronics & Communication Engineering Journal, 14*(5), 180-190.

Davis, D. (1996). Compliance defects in public-key cryptography. *In 6th USENIX security symp*, San Jose,CA, USA, 171-178.

Denzin, N. K., & Lincoln, Y. S. (2000). *Handbook of qualitative research* (2nd ed.). Thousand Oaks, Calif.: Sage Publications.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on, 22*(6), 644-654.

Eisinger, J., Winterer, P., & Becker, B. (2005). Securing wireless networks in a university environment. 312-316.

Feagin, J., Orum, A., & Sjoberg, G. (1991). *A case for case study*. Chapel Hill, NC: University of North Carolina Press.

Fokine, K. (2002). Key management in ad hoc networks. *M.S. Thesis, Linkoping University, Linkoping, Swede.*

Fumy, W., & Landrock, P. (1993). Principles of key management. *Selected Areas in Communications, IEEE Journal on, 11*(5), 785-793.

Gang Xu, & Iftode, L. (2004). Locality driven key management architecture for mobile ad-hoc networks. 436-446.

Garfinkel, S. (1995). *PGP: Pretty good privacy*O'Reilly & Associates.

Godber, A., & Dasgupta, P. (2002). Secure wireless gateway. *WiSE '02: Proceedings of the 3rd ACM workshop on wireless security,* Atlanta, GA, USA, 41-46. from http://doi.acm.org/10.1145/570681.570686

Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. *STOC '85: Proceedings of the seventeenth annual ACM*

symposium on theory of computing, Providence, Rhode Island, United States, 291-304. from http://doi.acm.org/10.1145/22145.22178

Gutmann, P. (2004). Simplifying public key management. *Computer*, *37*(2), 101-103.

Hadjichristofi, G. C., Adams, W. J., & Davis, N. J., IV. (2005). A framework for key management in mobile ad hoc networks. *2* 568-573 Vol. 2.

Harn, L., & Hung-Yu Lin. (1993). Key management for decentralized computer network services. *Communications, IEEE Transactions on*, *41*(12), 1777-1779.

Harris, S. (2003). *CISSP certification all-in-one exam guide* (2nd ed.). CA: McGraw-Hill.

He Ge. (2005). An efficient key management scheme for pervasive computing. 657-661.

Hongmei Deng, Mukherjee, A., & Agrawal, D. P. (2004). Threshold and identity-based key management and authentication for wireless ad hoc networks. *1* 107-111 Vol.1.

Housley, R., & Arbaugh, W. (2003). Security problems in 802.11-based networks. *Communications of the ACM*, *46*(5), 31-34.

Hu, Y., Johnson, D. B., & Perrig, A. (2002). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. 3-13.

Hu, Y., Perrig, A., & Johnson, D. B. (2002). Ariadne:: A secure on-demand routing protocol for ad hoc networks. *MobiCom '02: Proceedings of the 8th annual international conference on mobile computing and networking*, Atlanta, Georgia, USA, 12-23. from http://doi.acm.org/10.1145/570645.570648

Hubaux, J., Buttyan, L., & Capkun, S. (2001). The quest for security in mobile ad hoc networks. *MobiHoc '01: Proceedings of the 2nd ACM international symposium on mobile ad hoc networking \& computing*, Long Beach, CA, USA, 146-155.

ISO International Standard 7498-2. (1998). Open systems interconnection reference model - part 2: Security architecture.

Ito, T., Ohta, H., Matsuda, N., & Yoneda, T. (2005). A key pre-distribution scheme for secure sensor networks using probability density function of node deployment. *SASN '05: Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks*, Alexandria, VA, USA, 69-75. from http://doi.acm.org/10.1145/1102219.1102233

Jansen, W. A. (1993). A second look at the SDNS key management protocol. 74-81.

Jiang, T., & Li, Q. (2004). A secure routing protocol for mobile ad-hoc networks. *5* 2825-2829 vol.5.

Jolly, G., Kuscu, M. C., Kokate, P., & Younis, M. (2003). A low-energy key management protocol for wireless sensor networks. 335-340 vol.1.

Kahn, J. M., Katz, R. H., & Pister, K. S. J. (1999). Next century challenges: Mobile networking for \"Smart dust\". *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on mobile computing and networking*, Seattle, Washington, United States, 271-278. from http://doi.acm.org/10.1145/313451.313558

Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: A link layer security architecture for wireless sensor networks. *SenSys '04: Proceedings of the 2nd international conference on embedded networked sensor systems*, Baltimore, MD, USA, 162-175. from http://doi.acm.org/10.1145/1031495.1031515

Karnik, A., & Passerini, K. (2005). Wireless network security - a discussion from a business perspective. 261-267.

Kong, J., Zerfos, P., Luo,H. , S. Lu, & Zhang, L. (2001). Providing robust and ubiquitous security support for mobile ad-hoc networks. 251-260.

Kostas, T., Kiwior, D., Rajappan, G., & Dalal, M. (2003). Key management for secure multicast group communication in mobile networks. *2* 41-43 vol.2.

Krippendorff, K. (2004). *Content analysis : An introduction to its methodology* (2nd ed.). Thousand Oaks, Calif.: Sage Publications.

Labiod, H., & Duffau, R. (2004). KMS: A key management system for multi-provider interconnected wi-fi WLANs. *4* 2061-2066 Vol.4.

Leedy, P. D., & Ormrod, J. E. (2001). *Practical research: Planning and design* (7th ed.). Upper Saddle River, New Jersey: Prentice-Hall.

Lehane, B., Doyle, L., & O'Mahony, D. (2003). Shared RSA key generation in a mobile ad hoc network. *2* 814-819 Vol.2.

Lu, W. -., & Sundareshan, M. K. (1989). Secure communication in internet environments: A hierarchical key management scheme for end-to-end encryption. *Communications, IEEE Transactions on, 37*(10), 1014-1023.

Luo, H., & Lu, S. (2000). Ubiquitous and robust authentication services for ad hoc wireless networks. *Technical Report 200030, UCLA Computer Science Department,*

Luo, H., Zerfos, P., Kong, J., Lu, S., & Zhang, L. (2002). Self-securing ad hoc wireless networks. 567-574.

Manikopoulos, C., & Li Ling. (2003). Architecture of the mobile ad-hoc network security (MANS) system. *4* 3122-3127 vol.4.

Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. *MobiCom '00: Proceedings of the 6th annual international conference on mobile computing and networking*, Boston, Massachusetts, United States, 255-265. from http://doi.acm.org/10.1145/345910.345955

Merwe, J. v. d., Dawoud, D., & McDonald, S. (2005). Fully self-organized peer-to-peer key management for mobile ad hoc networks. *WiSe '05: Proceedings of the 4th ACM workshop on wireless security*, Cologne, Germany, 21-30. from http://doi.acm.org/10.1145/1080793.1080799

Michener, J. R., & Acar, T. (2000). Security domains: Key management in large-scale systems. *Software, IEEE, 17*(5), 52-58.

Michiardi, P., & Molva, R. (2002). CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. *Communication and Multimedia Security Conference*,

Mollin, R. A. (2003). *RSA and PUBLIC-KEY CRYPTOGRAPHY*. Florida: CHAPMAN & HALL/CRC.

National Institute of Standards and Technology. (2005). *Mobile ad hoc networks (MANETs).* Retrieved February 13, 2006 from http://w3.antd.nist.gov/wahn_mahn.shtml

Neuendorf, K. A. (2002). *The content analysis guidebook*. Thousand Oaks, Calif.: Sage Publications.

Neumann, P. G. (1997). Crypto key management. *Communications of the ACM, 40*(8), 136.

Olariu, S., Eltoweissy, M., & Younis, M. (2005). ANSWER: Autonomous wireless sensor network. *Q2SWinet '05: Proceedings of the 1st ACM international workshop on quality of service \& security in wireless and mobile networks*, Montreal, Quebec, Canada, 88-95. from http://doi.acm.org/10.1145/1089761.1089776

Papadimitratos, P., & Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. *SCS Communication SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002),*

Park, S. H., Ganz, A., & Ganz, Z. (1998). Security protocol for IEEE 802.11 wireless local area network. *Mob.Netw.Appl., 3*(3), 237-246.

Patton, M. (2002). *Qualitative research & evaluation methods* (3rd ed.)Sage Publications.

Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wirel.Netw., 8*(5), 521-534.

Polk, W. T., Hastings, N. E., & Malpani, A. (2003). Public key infrastructures that satisfy security goals. *Internet Computing, IEEE, 7*(4), 60-67.

Rabaey, J. M., Ammer, M. J., da Silva, J. L.,Jr, Patel, D., & Roundy, S. (2000). PicoRadio supports ad hoc ultra-low power wireless networking. *Computer, 33*(7), 42-48.

Rajaravivarma, V., Yi Yang, & Teng Yang. (2003). An overview of wireless sensor network and applications. 432-436.

Ramanujan, R., Ahamad, A., Bonney, J., Hagelstrom, R., & Thurber, K. (2000). Techniques for intrusion-resistant ad hoc routing algorithms (TIARA). *21st century military communications conference proceedings MILCOM 2000, oct 22-25 2000, 2* 660-664. from http://dx.doi.org/10.1109/MILCOM.2000.904011

Reiter, M. K., Franklin, M. K., Lacy, J. B., & Wright, R. N. (1996). The \Ω key management service. *CCS '96: Proceedings of the 3rd ACM conference on computer and communications security*, New Delhi, India, 38-47. from http://doi.acm.org/10.1145/238168.238184

Royer, E. M., & Chai-Keong Toh. (1999). A review of current routing protocols for ad hoc mobile wireless networks. *Personal Communications, IEEE [See also IEEE Wireless Communications], 6*(2), 46-55.

RuiYing Du, HuiJuan Tu, & Wen Song. (2005). An efficient key management scheme for secure sensor networks. 279-283.

Sass, P. (1999). Communications networks for the force XXI digitized battlefield. *Mob.Netw.Appl., 4*(3), 139-155.

Schmidt, T., & Townsend, A. (2003). Why wi-fi wants to be free. *Communications of the ACM, 46*(5), 47-52.

Seys, S., & Preneel, B. (2005). The wandering nodes: Key management for low-power mobile ad hoc networks. 916-922.

Stake, R. E. (1995). *The art of case study research*. Thousand Oaks, CA: Sage Publications.

Suen, T., & Yasinsac, A. (2005). Ad hoc network security: Peer identification and authentication using signal properties. 432-433.

Tellis, W. (1997). *Application of a case study methodology.* No. 3(3)The Qualitative Report.

Tie, L., & Li, J. (2005). Combinatorial optimization for wireless sensor networks. 439-442.

Tseng, Y. (2003). A scalable key-management scheme with minimizing key storage for secure group communications. *Int.J.Netw.Manag., 13*(6), 419-425.

Weber, R. P. (1990). *Basic content analysis* (2nd ed.)Sage university papers series. Quantitative applications in the social sciences ; no. 07-049.

Witzke, E. L., & Pierson, L. G. (1994). Key management for large scale end-to-end encryption. 76-79.

Xie, B., & Kumar, A. (2004). A framework for integrated internet and ad hoc network security. *1* 318-324 Vol.1.

Yan Sun, Trappe, W., & Liu, K. J. R. (2004). A scalable multicast key management scheme for heterogeneous wireless networks. *Networking, IEEE/ACM Transactions on, 12*(4), 653-666.

Yang, H., Meng, X., & Lu, S. (2002). Self-organized network-layer security in mobile ad hoc networks. *WiSE '02: Proceedings of the 3rd ACM workshop on wireless security*, Atlanta, GA, USA, 11-20. from http://doi.acm.org/10.1145/570681.570683

Yi, P., Yao, Y., Hou, Y., Zhong, Y., & Zhang, S. (2004). Securing ad hoc networks through mobile agent. *InfoSecu '04: Proceedings of the 3rd international conference on information security*, Shanghai, China, 125-129. from http://doi.acm.org/10.1145/1046290.1046315

Yi, S., Naldurg, P., & kravets, R. (2002). A security-aware ad hoc routing protocol for wireless networks. *6th World Multi-Conference on Systemic, Cybernetics and Informatics (SCI 2002),*

Yi, S., & Kravets, R. (2004). Composite key management for ad hoc networks. 52-61.

Yi, S., & Kravets, R. (2002). Key management for heterogeneous ad hoc wireless networks. 202-203.

Yi, S., Naldurg, P., & Kravets, R. (2001). Security-aware ad hoc routing for wireless networks. *Proceedings of the 2001 ACM international symposium on mobile ad hoc networking and computing: MobiHoc 2001, oct 4-5 2001*, 299-302. from http://dx.doi.org/10.1145/501416.501464

Yin, R. K. (2003). *Case study research* (3rd ed.). Thousand Oaks: Sage Publications.

Zhang, Q., & Wang, Y. (2004). A centralized key management scheme for hierarchical access control. *4* 2067-2071 Vol.4.

Zhang, Y., & Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. *MobiCom '00: Proceedings of the 6th annual international conference on mobile computing and networking*, Boston, Massachusetts, United States, 275-283. from http://doi.acm.org/10.1145/345910.345958

Zhen Yu, & Yong Guan. (2005). A robust group-based key management scheme for wireless sensor networks. *4* 1915-1920 Vol. 4.

Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. *Network, IEEE, 13*(6), 24-30.

Vita

Captain Yongjoo Shin is a member of Republic of Korea Army (ROKA). He graduated from Mae-San High School in Sun-Cheon, Korea in 1996. He attended the Korea Military Academy in Seoul, Korea where he received his Bachelor of Science Degree in Engineering Sciences in March 2000. After graduation, he was commissioned as Communication Officer and attended the Officer Basic Course of Communication branch.

His first active duty assignment was in the 3rd Infantry Division in Chul-Won, Korea. At that time, he managed the wireless network in his division. In May 2001, he applied for a position as Computer Officer and entered the Basic Officer Course for Computer Officer. After graduating he was assigned to the Head Quarter of Army in Dae-Jeon, Korea. During these 2 years, he worked as computer officer and managed a large database. In June 2003, he was selected to pursue a Master of Degree in the United States of America.

In August 2004 he entered the Air Force Institute of Technology at Wright Patterson Air Force Base to earn a Master of Science Degree in Information Systems Management. Upon graduation, he will be assigned to the Communication School in Dae-Jeon, Korea and attend the Officer Advanced Course in support of the mission of his Company Command. Upon completion of the course, he will be assigned to Communication Company Command.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
23-03-2006	**Master's Thesis**	Aug 2004 – Mar 2006

4. TITLE AND SUBTITLE

Factors Impacting Key Management Effectiveness in Secured Wireless Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Shin, Yongjoo, Captain, ROKA

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/06M-09

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The use of a Public Key Infrastructure (PKI) offers a cryptographic solution that can overcome many, but not all, of the MANET security problems. One of the most critical aspects of a PKI system is how well it implements Key Management. Key Management deals with key generation, key storage, key distribution, key updating, key revocation, and certificate service in accordance with security policies over the lifecycle of the cryptography. The approach supported by traditional PKI works well in fixed wired networks, but it may not appropriate for MANET due to the lack of fixed infrastructure to support the PKI. This research seeks to identify best practices in securing networks which may be applied to new network architectures.

15. SUBJECT TERMS
Key management, wireless network security, problems of key management

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Dr. Michael R. Grimaila (ENV)
U	**U**	**U**	**UU**	117	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 4800; e-mail: Michael.Grimaila@afit.edu