ABSTRACT

MULTILEVEL ADAPTIVE SECURITY SYSTEM

by
Hongwei Li

Recent trends show increased demand for content-rich media such as images, videos and text in ad-hoc communication. Since such content often tends to be private, sensitive, or paid for, there exists a requirement for securing such information over resource constrained ad hoc networks. In this work, traditional data security mechanisms, existing ad hoc secure routing protocols and multilevel security are first reviewed. Then a new system, called the Multilevel Adaptive Security System, which incorporates the multilevel security concept at both the application layer and the network layer, is proposed to provide adaptive security services for data and routing processes.

MLASS is composed of two subsystems: Content-Based Multi-level Data Security (CB-MLDS) for content-rich data protection and Multi-Level On-demand Secure Mobile Ad hoc Routing (MOSAR) for secure route selection. The structure of each sub-system is explained in detail; experiments for each sub-system were conducted and the performance was analyzed. It is shown that MLASS is a practical security solution that is flexible enough to adapt to a range of security requirements and applies appropriate level of security services to data and its distribution over ad hoc networks. MLASS provides a balance between security, performance and resource.

MULTILEVEL ADAPTIVE SECURITY SYSTEM

by
Hongwei Li

A Dissertation
Submitted to the Faculty of
New Jersey Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of
Doctor of Philosophy in Computer Engineering

Department of Electrical and Computer Engineering

January 2006

APPROVAL PAGE

MULTILEVEL ADAPTIVE SECURITY SYSTEM

Hongwei Li

Dr. Atam P. Dhawan, Dissertation Advisor — Date
Chair and Professor of Electrical and Computer Engineering, NJIT

Dr. Yunqing Shi, Committee Member — Date
Professor of Electrical and Computer Engineering, NJIT

Dr. Mengchu Zhou, Committee Member — Date
Professor of Electrical and Computer Engineering, NJIT

Dr. Constantine Manikopoulos, Committee Member — Date
Associate Professor of Electrical and Computer Engineering, NJIT

Dr. Qun Ma, Committee Member — Date
Assistant Professor of Computer Science, NJIT

Dr. Roberto Rojas-Cessa, Committee Member — Date
Assistant Professor of Electrical and Computer Engineering, NJIT

BIOGRAPHICAL SKETCH

Author: Hongwei Li

Degree: Doctor of Philosophy

Date: January 2006

Undergraduate and Graduate Education:

- Doctor of Philosophy in Computer Engineering,
  New Jersey Institute of Technology, Newark, NJ, 2006

- Master of Science in Computer Science,
  New Jersey Institute of Technology, Newark, NJ, 2002

- Bachelor of Science in Physics,
  Peking University, Beijing, P. R. China, 1992

Major: Computer Engineering

Presentations and Publications:

Hongwei Li and Atam Dhawan,
"Multilevel On-Demand Secure Ad Hoc Routing",
Submitted to Journal of Computer Security.

Hongwei Li and Atam Dhawan,
"Content-Based Multilevel Information Secure Distribution in Ad Hoc Networks",
Submitted to International Journal of Information Security.

Hongwei Li and Atam Dhawan,
"Agent Based Multilevel Dynamic Multimedia Security System",
Proceedings of 5th IEEE Systems, Man and Cybernetics Information Assurance Workshop, West Point, NY,
pp. 291-297, June 10-11, 2004.

Hongwei Li,
"Multilevel Dynamic Information Security System", Poster Presentation,
New Jersey Homeland Security Conference, hosted by US Army Fort Monmouth,
June 7, 2004.

This dissertation is dedicated to my beloved husband Mike, my caring parents, and my dear brother, for their unfailing support and love throughout my entire education.

谨以此论文献给我的爱人马跃，我敬爱的父母及哥哥和嫂子
以感谢他们对我无尽的爱和关怀

ACKNOWLEDGMENT

The journey here has not been easy since I started my Ph.D. study four years ago. Without the support of many people, this work, probably, would not have been possible. I am grateful to their kind support and encouragement. Here, I would like to express my gratitude to all of them.

I would like to express my deepest appreciation to my supervisor Dr. Atam Dhawan, who guided my research and led me all the way into this degree. Thank you for always believing in me and keeping me confident in my research.

Special thanks are given to my committee member Dr. Yunqing Shi, Dr. Mengchu Zhou, Dr. Constantine Manikopoulos, Dr. Roberto Rojas-Cessa and Dr. Qun Ma for taking their valuable time to attend my thesis defense and providing valuable advice on my final dissertation.

Many of my fellow graduate students in the Signal and Image Processing Research Laboratory deserve recognition for their support. I also want to thank Sachin and Song Wang for their assistance over the past few years.

My greatest thanks go to my beloved husband Mike for his patience and support while I was writing this thesis. I am grateful to my parents and family for always encouraging me to pursue my ideas and desires and for their unfailing support and love throughout my entire education.

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

Chapter **Page**

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES
(Continued)

CHAPTER 1

INTRODUCTION

1.1 Motivation

As the Internet and Intranet communication dominates in various government, business, industry and military application domains, security of data and communication protocols including routing has becomes a central issue and a critical challenge in the user community.

Recent trends show the increased demand for content-rich media such as images, videos and text in ad-hoc communication. Since such content often tends to be private, sensitive, or paid for, there exists a requirement for securing such information. Routing protocol supports the delivery of packets. Even with secure routing protocols, user's data is still at risk because once a document reaches its destination; it is no longer protected and can be accessed, changed, and distributed inappropriately by unauthorized users. Thus users' data needs to be protected by mechanisms that enforce a security and privacy policy. Routing is the fundamental part of network infrastructure, including wired and wireless networks. Network security has been the key issue for routing secured communication with a significant operational impact in application domains.

For wired networks, several secured routing protocols have been proposed. These protocols include routing information protocol (RIP), open shortest path first (OSPF), as well as border gateway routing protocol (BGP). The security mechanisms used in these protocols vary from the simple password based schemes to the complex digital signatures.

For mobile ad hoc networks (MANET), a robust and efficient secured routing is particularly a difficult task due to dynamic nature of the routing system. Ad hoc networks have no pre-deployed infrastructure available for routing packets end-to-end in a network. Nodes communicate with each other without the intervention of centralized access points or base stations, so each node acts both as a router and as a host. The emergence of such new networking approaches sets new challenges even for the fundamentals of routing, since the mobile ad-hoc networks are significantly different from the traditional networks. Several routing protocols, i.e. Ad-Hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR), which cope well with the dynamic nature of ad hoc networks, have been proposed, but the security issues have been initially left for small notice [1]. Most of these routing protocols take security for granted and assume that every node in the environment is cooperative and trustworthy. This blind trust model allows malicious nodes to attack an ad hoc network by means such as inserting erroneous routing updates, adverting incorrect routing information, and etc. While these attacks are possible in wired networks as well, the nature of ad hoc environment magnifies their effects, and makes their detection difficult.

Recently, a significant effort has been dedicated to the development of ad hoc secure routing protocols [2]. As a result, there are a number of secure routing protocols, such as ARAN (Authenticated Routing for Ad hoc Networks) and Ariadne, available for MANET today [3, 4]. In order to protect data from being attacked during the transmission over the ad hoc networks, the MANET routing protocols must be secured from the viewpoint of the authentication, integrity, non-repudiation, privacy and authority. The recent developments to achieve this task still lack in providing efficient and robust

performance particularly when the user network grows and involves different levels of security needs.

Traditionally, security systems are designed using a fixed template. That is, the same security services are applied to user's data without considering the difference in the sensitivity of data. However, solutions that rely only on traditional security mechanisms are unsuitable for resource-constrained ad hoc networks. This inflexibility of the traditional security mechanisms implies two main disadvantages for ad hoc networks: for highly sensitive data, the security offered by the fixed template may be inadequate to protect the data from being attacked; and for data with low security requirement, the fixed security template impacts the effectiveness of the network due to the cost of unnecessary security mechanisms. The disadvantages are magnified in mobile ad hoc networks, where are characterized as limited bandwidth, dynamic topology, lack of link or network-level security.

Therefore, in MANET networks, various security mechanisms should be implemented at several layers. In this research project, a new security system is proposed that integrates multi-level security concept to provide combined security operations to prevent user's original data and the MANET routing mechanisms from being accessed or modified by unauthorized nodes. This system is flexible enough to adapt to a range of security requirements, thus provides appropriate level of security services to the data distributed over MANET networks.

1.2 Problem Statement and Objectives

Organizations in the distributed environment must have the ability to quickly achieve higher, more refined levels of security data control for better adherence to the continuously changing nature of organizational rules. Multilevel security is the ability to distinguish subjects according to classification levels, which determines the degree to which they can access confidential objects. In the case of groups, this means that some members can exchange messages at a higher sensitivity level than others.

A multi-level secure (MLS) network is one where a single network is used to communicate data at different sensitivity levels (e.g. Unclassified and Secret). Many governments have significant interest in MLS networking. MLS networking requires the use of strong mandatory access controls which ordinary users are incapable of controlling or violating. In Mandatory access control policies a subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level [5].

A variant of these policies could be implemented for certain scenario's where an object needs to have multiple levels of access and an existing application provides no inherent means to support it. Multicasting, as an efficient way to deliver real time data to a large group of users in mobile ad hoc networks, is one of such cases. Moreover, the necessary security features such as data confidentiality, source/group authentication etc., are not readily offered by current ad hoc multicast routing protocols.

This could be illustrated in a situation like when a general would want to share information, such as image, video, audio, or text, with his subordinates. Some information that has UNCLASSIFIED nature would be shared with everyone in his distribution list and also some TOP SECRET information could only be shared among a group of officers. In addition, multi-level security in an ad hoc network at the routing level is necessary. Consider the following scenario [6]. The general detects that some of the privates have been compromised. He decides that he can only trust nodes owned by officers to route his SECRET packets. Thus in the general's route discover protocol, security level is used as a metric to establish the route. As shown in Figure 1.1, instead of the shortest route, a route with higher security level is formed by the nodes meet the security requirements embed in the general's route request packets. Only these nodes may respond and forward the packets.

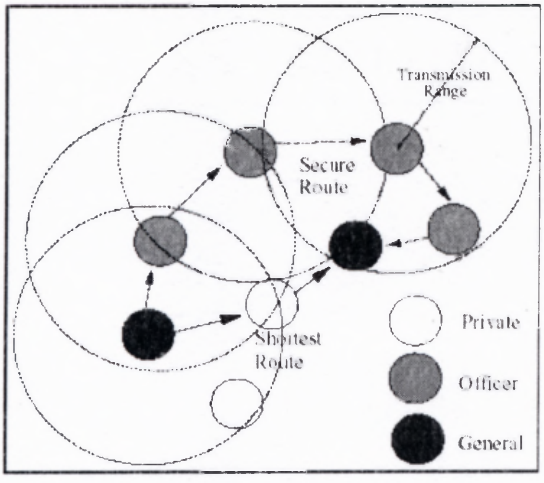

Figure 1.1 Multi-Level Secure Routing.

Though there have been some recent research publications, most of them address multiple levels of data security with respect to a network. There is no other research work that addresses the feasibility and performance measures of a multilevel adaptive security

system, involving multiple levels of data and routing security being transmitted through the network at the same time. This dissertation presents a system, Multi-Level Adaptive Security System (MLASS), which is capable of dealing with multilevel data and mobile ad hoc routing security and examines its feasibility for performance evaluation with single level security systems. The objectives of this research work are:

- To explain the structure of MLASS that deploys multi-level security technology, cryptography and steganography to provide adaptable and flexible security services for data and its distribution;
- To construct the secure content-based data processing subsystem that provides multi- level security services to the data being distributed;
- To integrate multi-level security with ad-hoc routing protocol and verify the feasibility of the new scheme;
- To analyze the performance of the proposed approach.

1.3 Organization of the Report

MLASS is a tool kit that provides the ability to properly label security-level, based on the security requirements, to different parts of a document, and offer corresponding security services to protect each part of the data and its distribution. In chapter 2, chapter 3 and chapter 4, an overview on data security, ad hoc network routing security and multi-level security technology is given respectively; in chapter 5, the architecture of MLASS and the methodology used to develop the proposed system are explained in detail; and in chapter 6, the experiment results are demonstrated and the performances are analyzed; conclusions are given in chapter 7 and future work is described in chapter 8.

CHAPTER 2

OVERVIEW OF DATA SECURITY

2.1 Classification of Data Security Services

As information systems become ever more pervasive and essential to the conduct of our affairs, electronic information takes on many of the roles traditionally performed by paper documents. Accordingly, the types of functions traditionally associated with paper documents must be performed on documents that exist in electronic form. The security services required to protect data are listed below [7].

- Confidentiality -- Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.
- Authentication -- Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
- Integrity -- Ensures that only authorized parties are able to modify computer systems assets and transmitted information.
- Non-repudiation -- Requires that neither the sender nor the receiver of a message be able to deny the transmission.
- Access control -- Requires that access to information resources may be controlled by or for the target system.
- Availability -- Requires that computer system assets be available to authorized parties when needed.

2.2 Security Attacks

There are four generic types of attack that might be encountered in the real world [7].

- Interruption -- An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include destruction of piece of hardware, or the disabling of the file management system.

- Interception -- An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program, or a computer. Example includes the illicit copying of files or programs.

- Modification -- An unauthorized party not only gains access to but also tampers with an asset. This is an attack on integrity. Examples include changing values in a data file, and modifying the content of messages being transmitted in a network.

- Fabrication -- An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. Example includes the addition of records to a file.

2.3 Data Security Mechanisms

2.3.1 Cryptography in Data Security

Cryptography not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below.

2.3.1.1 Secret Key Cryptography. With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher-text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. With this form of cryptography, it is obvious that the

key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach is the distribution of the key.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher-text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher-text in a stream cipher.

Block ciphers can operate in one of several modes [7]:

- Electronic Codebook (ECB) mode is the simplest, most obvious application: the secret key is used to encrypt the plaintext block to form a cipher-text block. Two identical plaintext blocks, then, will always generate the same cipher-text block. Although this is the most common mode of block ciphers, it is susceptible to a variety of brute-force attacks.

- Cipher Block Chaining (CBC) mode add a feedback mechanism to the encryption scheme. In CBC, the plaintext is exclusively-ORed (XORed) with the previous cipher-text block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same cipher-text.

- Cipher Feedback (CFB) mode is a block cipher implementation as a self-synchronizing stream cipher. CFB mode allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input. Output Feedback (OFB) mode is a block cipher implementation conceptually similar to a synchronous stream cipher. OFB prevents the same plaintext block from generating the same cipher-text block by using an internal feedback mechanism that is independent of both the plaintext and cipher-text bit-streams.

Secret key cryptography algorithms that are in use today include:

- Data Encryption Standard (DES) -- DES is the most common SKC scheme used today. DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks. DES has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations. Triple-DES (3DES) and DESX are two important variants that strengthen DES.

- Advanced Encryption Standard (AES) -- AES uses an SKC scheme called Rijndael. The algorithm can use a variable block length and key length; the latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits.

- CAST-128/256 -- CAST-128 is a DES-like substitution-permutation crypto algorithm, employing a 128-bit key operating on a 64-bit block. CAST-256 is an extension of CAST-128, using a 128-bit block size and a variable length (128, 160, 192, 224, or 256 bit) key. CAST-256 was one of the Round 1 algorithms in the AES process.

- International Data Encryption Algorithm (IDEA) -- IDEA is a 64-bit SKC block cipher using a 128-bit key.

- RC4/RC5/RC6 -- RC4 is a stream cipher using variable-sized keys; it is widely used in commercial cryptography products, although it can only be exported using keys that are 40 bits or less in length. RC5 is a block-cipher supporting a variety of block sizes, key sizes, and number of encryption passes over the data. RC6 is an improvement over RC5. RC6 was one of the AES Round 2 algorithms.

- Blowfish -- Blowfish is a symmetric 64-bit block cipher; optimized for 32-bit processors with large data caches, it is significantly faster than DES on a Pentium/PowerPC-class machine. Key lengths can vary from 32 to 448 bits in length.

- Twofish -- Twofish is a 128-bit block cipher using 128-, 192-, or 256-bit keys. Designed to be highly secure and highly flexible, well suited for large microprocessors, 8-bit smart card microprocessors, and dedicated hardware. It was one of the Round 2 algorithms in the AES process.

2.3.1.2 Public-Key Cryptography. Public-key cryptography depends upon the existence of one-way functions, or mathematical functions that are easy to computer whereas their inverse function is relatively difficult to compute.

Generic PKC employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the cipher-text. Because a pair of keys is required, this approach is also called asymmetric cryptography.

In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the *private key* and is never revealed to another party. It is straightforward to send messages under this scheme. Suppose Alice wants to send Bob a message. Alice encrypts some information using Bob's public key; Bob decrypts the cipher-text using his private key. This method could be also used to prove who sent a message; Alice, for example, could encrypt some plaintext with her private key; when Bob decrypts using Alice's public key, he knows that Alice sent the message and Alice cannot deny having sent the message.

Public-key cryptography algorithms that are in use today for key exchange or digital signatures include [7]:

- RSA -- It is the most common PKC implementation. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n (and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure.

- Diffie-Hellman -- D-H is used for secret-key key exchange only, and not for authentication or digital signatures.

- Digital Signature Algorithm (DSA) -- The algorithm provides digital signature capability for the authentication of messages.

- ElGamal -- It is a PKC system similar to Diffie-Hellman and used for key exchange.

- Elliptic Curve Cryptography (ECC) -- A PKC algorithm based upon elliptic curves. ECC can offer levels of security with small keys comparable to RSA and other PKC methods. It was designed for devices with limited compute power and/or memory, such as smart cards and PDAs.

2.3.1.3 Hash Functions. Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's content, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, help preserve the integrity of a file.

Hash algorithms that are in common use today include [7]:

- Message Digest (MD) algorithms -- A series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message.

- MD2/MD4/MD5 -- MD2 is designed for systems with limited memory, such as smart cards. MD4 is similar to MD2 but designed specifically for fast processing in software. MD5 is an improvement to MD4 but is slower because more manipulation is made to the original data. MD5 has been implemented in a large number of products although several weaknesses in the algorithm were demonstrated by German cryptographer Hans Dobbertin in 1996.

- Secure Hash Algorithm (SHA) -- SHA-1 produces a 160-bit hash value. SHA-224, SHA-256, SHA-384, and SHA-512 can produce hash values that are 224, 256, 384, or 512 bits in length, respectively.

- RIPEMD -- It is a series of message digests that initially came from the RIPE. RIPEMD-160 was optimized for 32-bit processors to replace the then-current 128-bit hash functions. Other versions include RIPEMD-256, RIPEMD-320, and RIPEMD-128.

- HAVAL (HAsh of VAriable Length) -- HAVAL is a hash algorithm with many levels of security. HAVAL can create hash values that are 128, 160, 192, 224, or 256 bits in length.

2.3.1.4 Combination of Cryptographic Schemes. Each of the three cryptographic schemes is optimized for some specific application(s). Hash functions, for example, are well suited for ensuring data integrity because any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. Since it is highly unlikely that two different messages will yield the same hash value, data integrity is ensured to a high degree of confidence.

Secret key cryptography, on the other hand, is ideally suited to encrypting messages. The sender can generate a *session key* on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message.

Key exchange, of course, is a key application of public-key cryptography. Asymmetric schemes can also be used for non-repudiation; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message. Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography.

2.3.2 Steganography

Secret communication is essential for security. Hidden information has a variety of uses in products and protocols. For example, hidden information can be used as document authentication or private communication. There are a number of different ways to hide information [8].

- Use the noise -- The simplest technique is to replace the noise in an image or sound file with user's message. A digital file consists of numbers that represent the intensity of light or sound at a particular point in time or space. Often, these numbers are computed with extra precision that can't be detected effectively by humans. User's message can be hidden in the least significant bits for each color of each pixel. The human eye would not be able to detect the subtle variations, but a computer could reconstruct all of it.

- Spread the information out -- Some of the more sophisticated mechanisms spread the information out over a number of pixels or moments in a sound file. This diffusion protects the information and also makes it less susceptible to detection, either by humans looking at the information or by computers looking for statistical profiles. Spreading the information out often increases the resilience to destruction by either random or malicious forces. The spreading algorithms often distribute the information in such a way that not all of the bits are required to reassemble the original data. If some parts get destroyed, he message still gets through.

- Replace randomness -- Many software programs use random number generators to add realism to scenes, sounds, and games. Information can be hidden in the place of the random number.

- Change the order -- A grocery list may be just a list, but the order of the items can carry a surprisingly large amount of information.

- Split information -- There is no reason why the data needs to travel in one package. Data can be split into any number of packets that take different routes to their destination. Sophisticated algorithms can also split the information so that any subsets of k of the n parts are enough to reconstruct the entire message.

CHAPTER 3

OVERVIEW OF AD HOC ROUTING SECURITY

Ad Hoc network is a set of wireless mobile nodes forming a dynamic autonomous network through a fully mobile infrastructure. Nodes communicate with each other without the intervention of centralized access points or base stations, so each node acts both as a router and as a host.

In the traditional Internet, routers within the central parts of the network are owned by a few well-known operators and are therefore assumed to be somewhat trustworthy. This assumption no longer holds in an Ad Hoc network since all nodes entering the network are expected to take part in routing. Also, because the links are usually wireless, any security that was gained because of the difficulty of tapping into a network is lost. Furthermore, because the topology in such a network can be highly dynamic, traditional routing protocols can no longer be used [2]. Thus Ad Hoc network has much harder security requirements than the traditional network and the routing in Ad Hoc networks is an especially hard task to accomplish securely, robustly and efficiently.

Several Ad Hoc routing protocols have been proposed, which include AODV, DSR, ZRP, TORA, DSDV, STAR, and others. But all these protocols have security vulnerabilities and exposures, and can easily be attacked. The purpose of this section is to analyze the vulnerabilities of Ad Hoc routing and discuss the existing secure routing protocols.

3.1 Attacks to Ad Hoc Routing

3.1.1 Passive Attacks

Passive attacks typically involve unauthorized "listening" to the routing packets. That is, the attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routing traffic.

The major advantage for the attacker in passive attacks is that in a wireless environment the attack is usually impossible to detect. This also makes defending against such attacks difficult. Furthermore, routing information can reveal relationships between nodes or disclose their addresses. If a route to a particular node is requested more often than to other nodes, the attacker might expect that the node is important for the functioning of the network, and disabling it could bring the entire network down.

Other interesting information that is disclosed by routing data is the location of nodes. Even when it might not be possible to pinpoint the exact location of a node, one may be able to discover information about the network topology.

3.1.2 Active Attacks

To perform an active attack the attacker must be able to inject arbitrary packets into the network. The goal may be to attract packets destined to other nodes to the attacker for analysis or just to disable the network. A major difference in comparison with passive attacks is that an active attack can sometimes be detected. This makes active attacks a less inviting option for most attackers.

Some types of active attacks that can usually be easily performed against an ad hoc network include:

- Black Hole -- A malicious node uses the routing protocol to advertise itself as having the shortest path to nodes whose packets it wants to intercept. In a flooding based protocol such as AODV, the attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply where an extremely short route is advertised. If the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

- Rushing attack -- Some routing protocols such as AODV instantiate and maintain routes by assigning monotonically increasing sequence numbers to routes toward specific destinations. In AODV, any node may divert traffic through itself by advertising a route to a node with a destination sequence number greater than the authentic value [4]. Even the source node eventually receives the legitimate ROUTE REPLY (RREP) packets, it will discard those packets, thinking that the valid route is stale. Hence, the source node would not be able to find secure routes, that is, routes that do not include the adversary node.

- Wormhole attack -- In the wormhole attack, an attacker records packet at one location in the network, tunnels them to another location, and retransmits them from there into the network. Due to the broadcast nature of the radio channel, the attacker can create a wormhole even for packets not addressed to itself. If a wormhole attacker tunnels all packets through the wormhole honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently [4]. However, when an attacker forwards only routing control messages, this attack might severely disrupt routing. For example, when used against an on-demand routing protocol such as DSR or AODV, a powerful application of the wormhole attack can be mounted by tunneling each RREQ packet directly to the target node of the RREQ. This attack prevents any node from discovering routes more than two hops long.

- Spoofing attacks -- Spoofing occurs when a node misrepresents its identity in the network, such as by altering its MAC or IP address in outgoing packets [2]. By masquerading as another node, a malicious node can launch many attacks in a network. Spoofing combined with packet modification is really a dangerous attack, for example, it can cause routing loops in ad hoc networks.

- Route Error Fabrication -- AODV implements path maintenance to recover broken paths when nodes move. If the destination node or an intermediate node along an active path moves, the node upstream of the link break broadcasts a route error message to all active upstream neighbors. The node also invalidates the route for this destination in its routing table. The vulnerability is that routing attacks can be launched by sending false route error messages, causing other nodes delete the valid entry in their routing table, therefore disrupt the communications. Such attacks can be difficult to verify as invalid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted [4].

- Routing Table Overflow -- In a routing table overflow attack the attacker attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. Proactive routing algorithms attempt to discover routing information even before it is needed while a reactive algorithm creates a route only once it is needed. This property appears to make proactive algorithms more vulnerable to table overflow attacks. An attacker can simply send excessive route advertisements to the routers in a network. Reactive protocols, such as AODV on the other hand, do not collect routing data in advance.

- Sleep Deprivation Torture -- Usually, attack is practical only in Ad Hoc networks, where battery life is a critical parameter. Battery powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes, or by forwarding unnecessary packets to the node using, for example, a black hole attack. This attack is especially suitable against devices that do not offer any services to the network or offer services only to those who have some special credentials. Regardless of the properties of the services, a node must participate in the routing process unless it is willing to risk becoming unreachable to the network.

- Location Disclosure -- A location disclosure attack can reveal something about the locations of nodes or the structure of the network. The information gained might reveal which other nodes are adjacent to the target, or the physical location of a node. The attack can be as simple as using an equivalent of the trace route command on Unix systems. Routing messages are sent with inadequate hop-limit values and the addresses of the devices sending the ICMP error-messages are recorded. In the end, the attacker knows which nodes are situated on the route to the target node. If the locations of some of the intermediary nodes are known, one can gain information about the location of the target as well.

3.2 Proposed Ad hoc Secure Routing Protocols

3.2.1 Secure Routing Protocol (SRP)

Panagiotis Papadimitratos and Zygmunt Haas propose the Secure Routing Protocol [9], which can be used with DSR or the Interzone Routing Protocol in the Zone Routing Protocol (ZRP). SRP is designed as an extension header that is attached to ROUTE REQUEST (RREQ) and ROUTE REPLY (RREP) packets. SRP doesn't attempt to secure ROUTE ERROR (RERR) packets but instead delegates the route-maintenance function to the Secure Route Maintenance portion of the Secure Message Transmission protocol. SRP uses a sequence number in the RREQ to ensure freshness, but this sequence number can only be checked at the target. SRP requires a security association only between communicating nodes and uses this security association just to authenticate RREQ and RREP through the use of message authentication codes. At the target, SRP can detect modification of the RREQ, and at the source, SRP can detect modification of the RREP.

However, SRP doesn't attempt to prevent unauthorized modification of fields that are ordinarily modified in the course of forwarding these packets. For example, a node can freely remove or corrupt the node list of a RREQ packet that it forwards.

Because SRP requires a security association only between communicating nodes, it uses extremely lightweight mechanisms to prevent other attacks. For example, to limit flooding, nodes record the rate at which each neighbor forwards RREQ packets and gives priority to RREQ packets sent through neighbors that less frequently forward RREQ packets. Such mechanisms can secure a protocol when few attackers are present; however, such techniques provide secondary attacks, such as sending forged RREQ packets to reduce the effectiveness of a node's authentic RREQ. In addition, such

techniques exacerbate the problem of greedy nodes. For example, a node that doesn't forward RREQ packets ordinarily achieves better performance because it is generally less congested, and it doesn't need to use its battery power to forward packets originated by other nodes. In SRP, a greedy node retains these advantages and, in addition, gets a higher priority when it initiates route discovery.

SRP authenticates RREP from intermediate nodes using shared group keys or digital signatures. When a node with a cached route shares a group key with (or can generate a digital signature verifiable by) the initiator of the RREQ, it can use that group key to authenticate the RREP. The authenticator, which is either a message authentication code computed using the group key or a signature, is called the intermediate node reply token. The signature or MAC is computed over the cache RREP.

As mentioned earlier, SRP doesn't attempt to address the route-maintenance question. In SRP, multiple RREP are returned for each RREQ; nodes use secure message transmission (SMT) [10] to ensure successful delivery of data packets. In SMT, data messages are split into packets using secret sharing techniques so that if M out of N such packets are received, the message can be reconstructed.

3.2.2 SEAD

Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [11] is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, in spite of active attackers or compromised nodes in the network. The design of SEAD is based in part on the Destination-Sequenced Distance-Vector ad hoc network routing

protocol (DSDV). To support use of SEAD with nodes of limited CPU processing capability, and to guard against DoS attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, the efficient one-way hash functions are employed instead of using asymmetric cryptographic operations in the protocol.

In distance-vector routing, each router maintains a routing table listing all possible destinations within the network. Each entry in a node's routing table contains the address of some destination, the node's shortest known distance to the destination, and the address of the first hop on the shortest route to the destination. Each router forwarding a packet uses its own routing table to determine the next hop toward the destination.

To maintain the routing tables, each node periodically broadcasts a routing update containing the information from its own routing table. Each node updates its own table using the updates it hears so that its route for each destination uses as a next hop the neighbor that advertised the smallest metric in its update for that destination.

The primary improvement for ad hoc networks made in DSDV over standard distance vector routing is the addition of a sequence number in each routing table entry. Using this sequence number prevents routing loops caused by updates being applied out of order. This problem can be common over multi-hop wireless transmission because the routing information can spread along many different paths through the network.

Given an existing authenticated element of a one-way hash chain, we can verify elements later in the sequence of use within the chain (further on, in order of decreasing subscript). Each node in SEAD uses a specific single next element from its hash chain in each routing update that it sends about itself (metric 0). Based on this initial element, the

one-way hash chain conceptually provides authentication for the metric's lower bound in other routing updates for this destination; the authentication provides only a lower bound on the metric--that is, an attacker can increase the metric or claim the same metric, but can't decrease the metric.

3.2.3 Ariadne

Ariadne [3] is a secure on-demand routing protocol that withstands node compromise and relies only on highly efficient symmetric cryptography. Ariadne is based on DSR and uses with Tesla, an efficient broadcast authentication scheme that requires loose time synchronization. Ariadne discovers routes on-demand through route discovery and uses them to source route data packets to their destinations. Each forwarding node helps by performing route maintenance to discover problems with each selected route.

Ariadne employs a mechanism that lets the target verify the authenticity of the RREQ and an efficient per-hop hashing technique to verify that no node is missing from the node list in the RREQ. To convince the target of the legitimacy of each field in a RREQ, the initiator simply includes a message authentication code (MAC) computed with the shared secret key K_{SD} over unique data, for example, a timestamp. The target can easily verify the route request's authenticity and freshness using the shared key K_{SD}. A secondary requirement is that the target can authenticate each node in the node list of the RREQ so that it will return a RREP only along paths that contain legitimate nodes. Each hop authenticates the new information in the RREQ using its current Tesla key. The target buffers the RREP until intermediate nodes can release the corresponding Tesla

keys. The Tesla security condition is verified at the target, and the target includes a MAC in the RREP to certify that the security condition was met. One-way hash functions are used to verify that no hop was omitted, an approach is called per-hop hashing. To change or remove a previous hop, an attacker must either hear a RREQ without that node listed or must be able to invert the one-way hash function.

Route maintenance in Ariadne is based on DSR. A node forwarding a packet to the next hop along the source route returns a RERR to the packet's original sender if it is unable to deliver the packet to the next hop after a limited number of retransmission attempts. To prevent unauthorized nodes from sending RERR, the sender has to authenticate an RERR. Each node on the return path to the source forwards the ERROR. If the authentication is delayed, for example, when Tesla is used—each node that will be able to authenticate the ERROR buffers it until it can be authenticated.

Ariadne is vulnerable to an attacker that happens to be along the discovered route. To avoid the continued use of malicious routes, routes are selected based on their prior performance in packet delivery.

3.2.4 Authenticated Routing for Ad hoc Networks (ARAN)

Kimaya Sanzgiri and her colleagues [4] developed authenticated routing for ad hoc networks (ARAN), which is based on AODV. In ARAN, each node has a certificate signed by a trusted authority, which associates its IP address with a public key. ARAN is an on-demand protocol, broken up into route discovery and maintenance.

To initiate a route discovery, the initiator broadcasts a signed RREQ packet that includes the target, its certificate, a nonce, and a timestamp. The nonce and timestamp together ensure freshness when used in a network with a limited clock skew. Each node that forwards this RREQ checks the signature or signatures. If the signatures are valid, the forwarding node removes the last forwarder's signature and certificate, signs the original RREQ, and includes its own certificate. The node then broadcasts the RREQ. When the first RREQ from a route discovery reaches the target, the target signs a RREP and sends it to the node from which it received the RREQ. The RREP is forwarded in much the same way as the RREQ, except that each node unicasts the RREP to the node from which it received the RREQ.

In route maintenance, the intermediate node sends a RERR to the previous hop, indicating that the route has been broken. This RERR includes the source, destination, intermediate node certificate, and a nonce and timestamp generated by the intermediate node for freshness. This packet is forwarded unchanged to the source.

Because ARAN uses public-key cryptography for authentication, it is particularly vulnerable to DoS attacks based on flooding the network with bogus control packets for which signature verifications are required. As long as a node can't verify signatures at line speed, an attacker can force that node to discard some fraction of the control packets it receives.

3.2.5 SAODV

Manel Guerrero Zapata and N. Asokan [12] propose Secure AODV (SAODV), another protocol designed to secure AODV. The idea behind SAODV is to use a signature to authenticate most fields of a RREQ and RREP and to use hash chains to authenticate the hop count. SAODV designs signature extensions to AODV. In SAODV, an RREQ packet includes a route request single signature extension (RREQ-SSE). The initiator chooses a maximum hop count, based on the expected network diameter, and generates a one-way hash chain of length equal to the maximum hop count plus one. This one-way hash chain is used as a metric authenticator. The initiator signs the RREQ and the anchor of this hash chain; both this signature and the anchor are included in the RREQ-SSE. In addition, the RREQ-SSE includes an element of the hash chain based on the actual hop count in the RREQ header. With the exception of the hop-count field and hop-count authenticator, the fields of the RREQ and RREQ-SSE headers are immutable and therefore can be authenticated by verifying the signature in the RREQ-SSE extension. To verify the hop-count field in the RREQ header, a node can follow the hash chain to the anchor.

When forwarding an RREQ in SAODV, a node first authenticates the RREQ to ensure that each field is valid. It then performs duplicate suppression to ensure that it forwards only a single RREQ for each route discovery. The node then increases the hop-count field in the RREQ header, hashes the hop count authenticator, and rebroadcasts the RREQ, together with its RREQ-SSE extension.

When the RREQ reaches the target, the target checks the authentication in the RREQ-SSE. If the RREQ is valid, the target returns an RREP as in AODV. A route reply single signature extension (RREP-SSE) provides authentication for the RREP. As in the

RREQ, the only mutable field is the hop count; as a result, the RREP is secured in the same way as the RREQ. In particular, an RREP-SSE has a signature covering the hash chain anchor together with all RREP fields except the hop count. The hop count is authenticated by a hop-count authenticator, which is also a hash chain element.

A node forwarding an RREP checks the signature extension. If the signature is valid, then the forwarding node sets its routing table entry for the RREP's original source, specifying that packets to that destination should be forwarded to the node from which the forwarding node heard the RREP.

SAODV allows intermediate-node replies through the use of a route reply double signature extension (RREP-DSE). An intermediate node replying to an RREQ includes an RREP-DSE. The idea here is that to establish a route to the destination, an intermediate node must have previously forwarded an RREP from the destination. If the intermediate node had stored the RREP and signature, number in that RREP is greater than the sequence number specified in the RREQ. However, some of the fields of that RREP, in particular the lifetime field, are no longer valid. As a result, a second signature, computed by the intermediate node, is used to authenticate this field.

To allow replies based on routing information from an RREQ packet, the initiator includes a signature suitable for an RREP packet through the use of an RREQ-DSE. Conceptually, the RREQ-DSE is an RREQ and RREP rolled into one packet. To reduce overhead, SAODV uses the observation that the RREQ and RREP fields substantially overlap. In particular, the RREQ-DSE need only include some flags, a prefix size, and some reserved fields, together with a signature valid for an RREP using those values.

When a node forwards an RREQ-DSE, it caches the route and signature in the same way as if it had forwarded an RREP.

SAODV also uses signatures to protect the route error (RERR) message used in route maintenance. In SAODV, each node signs the RERR it transmits, whether it's originating the RERR or forwarding it. Nodes implementing SAODV don't change their destination sequence number information when receiving an RERR because the destination doesn't authenticate the destination sequence number.

3.2.6 Security-Aware Routing (SAR)

In Security-Aware Routing (SAR) [6], the nodes in a network have different security attributes and are classified into different trust levels. The nodes of same trust level share a secret key. Routing is to find the nodes that match particular security attributes and trust levels. Security metrics are embedded into the routing request packet, and change the forwarding behavior of the protocol with respect to routing request packets. All routing request packets and routing reply packets are encrypted by the keys shared in the same level. Only nodes that provide the required level of security can generate or propagate route requests, updates, or replies.

SAR has a main problem. One is the restriction that a node, no matter its security clearance, only can send route request within the same trust level, which sometimes results in no qualified route being found, thus packets can not be delivered successfully. Such problem becomes more obvious for nodes with higher trust level, at which usually has less number of nodes assigned.

3.2.7 Open Research Challenges

A number of challenges remain in the area of securing wireless ad hoc networks [13]. First, the secure routing problem in such networks isn't well modeled. A more complete model of possible attacks would let protocol designers evaluate the security of their routing protocol. In addition, such a model would form the basis for using formal methods to verify protocol security.

Another problem is designing efficient routing protocols that have both strong security and high network performance. Although researchers have designed security extensions for several existing protocols, many of these extensions remove important performance optimizations. Optimistic approaches can provide a better tradeoff between security and performance.

CHAPTER 4

REVIEW ON MULTILEVEL SECURITY (MLS)

Multi-Level Security is defined as a class of systems containing information with different sensitivities that simultaneously permits access by users with different security level without the risk of compromise. DISA (Defense Information System Agency) Home Page defines Multi-Level Security as [5]:

- Allows information about different sensitivities (classifications) to be stored in an information system.
- Allows users having different clearances, authorizations, and need to know the ability to process information in the same system.
- Prevents users from accessing information for which they are not cleared, do not have authorization, or do not have a need to know.

In the United States military, these degrees are hierarchical in nature and, listed from least secure to most secure, are known as RESTRICTED, CONFIDENTIAL, SECRET, and TOP SECRET (Figure 4.1).

The most widely recognized approach to MLS is the Bell-LaPadula security model, which reflects the information flow restrictions inherent in the access restrictions applied to classified information. This model enforces MLS access restrictions by implementing two simple rules: the simple security property and the *-property.

- *Simple Security Property*: A subject can read from an object as long as the subject's security level is the same as, or higher than, the object's security level. This is sometimes called the no read up property.
- **-Property*: A subject can write to an object as long as the subject's security level is the same as or lower than the object's security level. This is sometimes called the no write down property.

The first rule enforces the access restriction on the need-to-know basis; and the second rule prevents information leakage from high level to low level. When a subject tries to read from or write to an object, the system compares the subject's security label with the object's label and applies these rules. Figure 4.2 [14] illustrates an example of above rules.

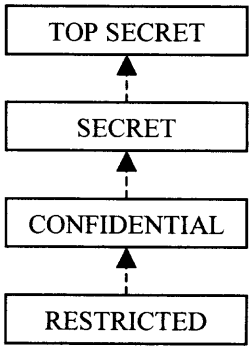

Figure 4.1 Security hierarchy.

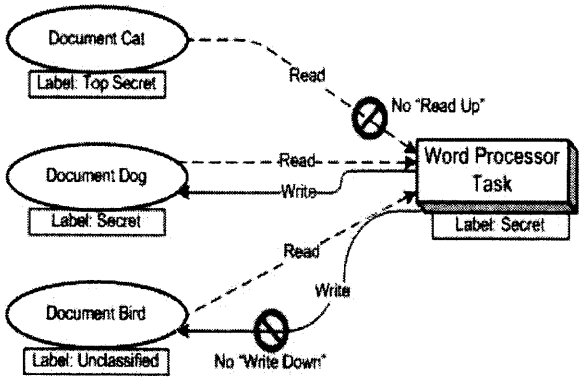

Figure 4.2 Data flows in LaPadula model.

The research on Multilevel Security technology has been ongoing for many years. Multi-Level Security Systems overcome the operational limitations imposed by system-high operations and are considered the most secured and effective system. The biggest advantage of MLS Systems is that it allows users at each security level to receive appropriate information and multimedia updates in real time, which would be difficult without this architecture. Each user has the access to the data that is appropriate for his/her security level. MLS guards and MLS workstations can be used to bridge security boundaries between existing single-level systems. MLS operating systems, MLS database management systems, and MLS networks can provide common data processing and data transfer platforms to serve as the foundation for MLS systems.

4.1 MLS Operating Systems

Developed in the early 1980s and begun to receive National Security Agency (NSA) evaluation in 1984, MLS operating systems provide complete mandatory and discretionary access control, thorough security identification of data devices, rigid control of transfer of data and access to devices, and complete auditing of access to the system and data. [5]

By implementing MLS operating system, security administrator is able to configure security clearance definitions and limitations, permitted special operational capabilities, file access control lists, and choice of password protection scheme. MLS operating systems provide security mechanisms and services that allow a computer system to distinguish and separate classified data and protect it against a malicious user's abuse of authority, direct probing, and human error.

MLS operating systems lower the security risk of implementing a system that processes classified data. They implement security policies and accountability mechanisms in an operating system package. A security policy is the rules and practices that determine how sensitive information is managed, protected, and distributed. Accountability mechanisms are the means of identifying and tracing who has had access to what data on the system so they can be held accountable for their actions.

4.2 MLS Database Management Systems (MLS DBMS)

A multilevel secure database management system is designed to archive, retrieve and process information in compliance with certain mandatory security requirements that are essential for protecting sensitive information from unauthorized access, modification and abuse.

Conventional database management systems treat all data at the same security level and ignore the actual security levels of the data they store and retrieve. Multi-Level Secure DBMS schemes provide a means of maintaining a collection of data with mixed security levels. The accessing mechanisms allow users or programs with different levels of security clearance to operate only the data that is appropriate to their levels.

Since 1975, research effort has been focused on the development of MLS DBMS. Many MLS DBMS architectures have been proposed, such as trusted subject architecture, the integrity lock architecture, the kernelized architecture, the replicated architecture, and the distributed architecture [15, 16, 17].

Different architectures suit different needs. The Trusted Subject architecture is best for applications where the trusted operating system and the hardware used in the architecture already provide an assured, trusted path between applications and the DBMS. The Integrity Lock architecture provides the ability to label data down to the row (or record) level, the ability to implement a wide range of categories, and is the easiest to validate. The Kernalized architecture scheme is economical and easier to implement for MLS DBMS systems with simple table structures. The Distributed architecture is desirable for DBMS where physical separation of data by security level is required.

4.3 MLS Networks

Due to the distributed nature of network architecture, the high degree of openness of network medium, and the intensive need for sharing resources within the network, the protection mechanisms residing in the individual computers that prevent unauthorized access to the files become inadequate to ensure the security of communications across the network.

In MLS Network [14], the enforcement mechanism is embedded in the network interface devices, network front-end processors, switches, routers and gateways to enforce the security policy for the network, handling information at different security classification levels and serving users with different security clearances. It controls the access to network equipment for which some users may not have the clearance to use, and it controls the flow of information between various network devices to prevent unauthorized dissemination.

The authors introduced an implementation of MLS Network (MLN) in [14]. The network has both unclassified and secret gateways and routers. Each workstation labels data unclassified or secret and transmits information to the proper gateway and router. Each gateway has an internal unlabeled multilevel network interface card. The routers act as a firewall to protect the network from external attacks. Identification and authentication within the MLN is achieved through user identification and password.

4.4 MLS Transaction Processing

In recent years, research has been conducted considerably to develop the concurrency control techniques and commit protocols for MLS DBMS to ensure secure transaction processing. In MLS database, transactions and data are labeled with different security levels. Convert channels can cause the leakage of information from one level to another level. Therefore, synchronizing readers and writers in an MLS environment becomes the main concern of the secure transaction processing. The concurrency control protocol in MLS DBMS shall not only ensure correct execution of transaction, but also prevent the establishment of convert channel.

The secure transaction processing for popular MLS DBMS architectures, such as kernelized, replicated, and distributed architectures, has been developed. So do advanced transaction models such as workflows, long duration and nested models. The replicated approach constructs an MLS DBMS from single-level DBMS. The challenge is how to design a replica control protocol that will ensure one-copy serializability. In [22], the authors point out the technical challenges in multilevel secure transaction processing when they review the existing models in this area. The common solution is that transactions are submitted to a global transaction manager, and the global transaction manager routes the transactions to their sites of origin and propagates the update projections to each of the domination containers sequentially. Snapshot algorithms proposed for the kernelized architecture create and maintain a snapshot of data, which will be read by transactions. Transactions access data at their own level and at the current state of database.

4.5 MLS Web Server

Multi-Level Security Web Server is another emerging trend. MLS Web Server allows organizations to maintain a common data set on a single World Wide Web server that connects to multiple security domains/networks. This alleviates the need to maintain multiple servers and data sets, one for each domain or network. It allows a single, common data resource to support multiple organizations where there is a requirement to restrict access to information based upon organizational or privacy needs. By placing all data on a single MLS Web Server, the time consuming and costly task of maintaining a common and consistent data set on multiple disconnected servers is alleviated [19].

Using secure operating system, secure web server, and secure database technology, information on the server can be segregated and maintained by categories, classification levels, or organizations. Individual users and groups can either be granted or denied access to this information based upon their authorization level, which is assigned by the system's security officer or administrator. Data can be organized hierarchically, if so desired, allowing users to access multiple sets of data and other information at and below their authorization level.

4.6 Summary

Multi-Level Security technology is applied in various field, including operating system, database management system, network, as well as transaction processing and web server. Secure routing protocols for ad hoc networks are proposed to prevent and discover misbehaviors of ad hoc nodes. The common goals of these secure systems are to protect

data from malicious user, to process data in secure and appropriate means, to deliver data to the correct receiver without releasing any sensitive information, and to improve system efficiency.

However, the end user community found a number of cases where that the Bell-LaPadula model of information flow did not entirely satisfy their operational and security needs. One of the problems is that the systems tend to collect a lot of "over-classified" information. Once a user creates a document at a high security level, the document will have to retain that security level even if the user removes all sensitive information in order to create a less-classified or even unclassified document. In essence, end users often need a mechanism to "downgrade" information so its label reflected its lowered sensitivity. The downgrading problem becomes especially important in the systems which use highly classified intelligence data to produce tactical commands to be sent to combat units whose radios received information at lower level.

CHAPTER 5

MULTI-LEVEL ADAPTIVE SECURITY SYSTEM (MLASS)

5.1 System Outline

MLASS is designed to provide varying security services for data and its transmission in mobile ad-hoc network. It integrates multi-level security concept and technology into application layer and network layer. The system requires all nodes participating in an ad-hoc network have a correctly pre-assigned Read/Route clearance, based on their hierarchies or roles in the organization. It is assumed that a node with higher clearance is more secure and possesses more privilege. Also, all messages exchanged within the network are associated with a Read/Route level, which is assigned by the source originating the message on the basis of the sensitivity of the message and on the "need to know" basis. The source must be only allowed to originate a message at its current level or at a level that falls below in the hierarchy. The node with a certain clearance is only allowed to read messages marked with its assigned Read level or any level below it. Therefore, only the highest security level nodes in the network may be allowed to possess the highest read level and lowest route level thereby enabling them to read the messages of all levels and also route at any desired level.

Although above rules stick with "read-down" property of the Bell-LaPadula model, it does not adhere to the "write-up" property. The reason of making such modification is that communication with a subject at a lower clearance level is frequently a necessity. We notice that some important defense applications require a "write down" capability. For example, a user with Top Secret clearance may wish to send an innocuous but important announcement via email to her colleagues with Secret clearance. She

knows that the recipients are authorized to receive the message's contents, but with the restriction of no write down property, she can not distribute her email. Therefore, the practical systems may not entirely rely on the Bell-LaPadula mechanisms.

MLASS is composed of two subsystems: Content-Based Multi-level Data Security (CB-MLDS) for user's data protection and Multi-Level On-demand Secure Ad hoc Routing (MOSAR) for secure route selection. The structure of MLASS is described in Figure 5.1:

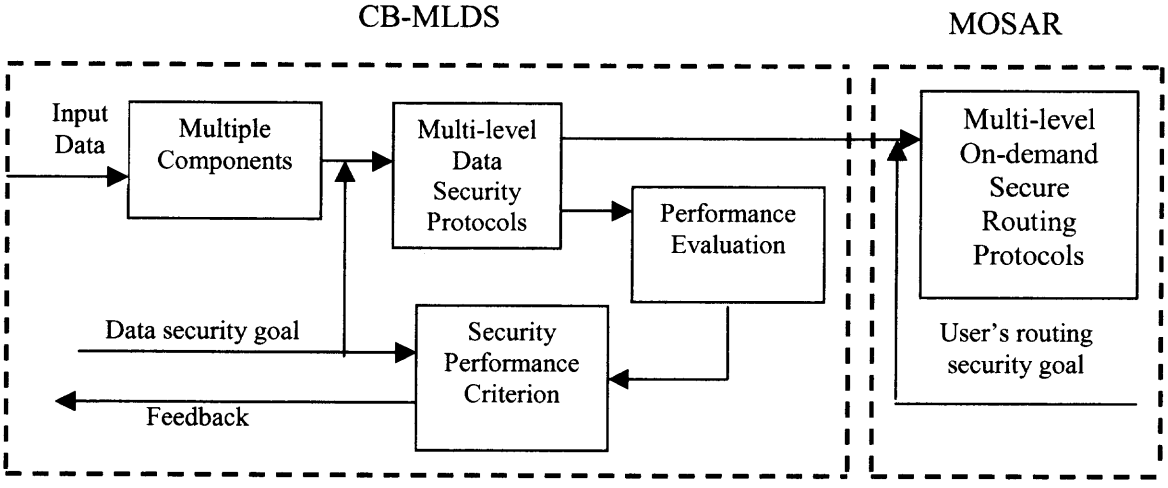

Figure 5.1 Architecture of MLASS.

It is common that a file consists of components with different sensitivity. For example, in identity recognition, human's face may disclose more information than the other parts of human's body. Similarly, the most significant bit-plane of an image contains much more information than the least significant bit-plane. Therefore, it is necessary to apply different protection mechanisms to each component for the purpose of security and efficiency. CB-MLDS is designed as the tool to help user decompose the original information into multiple sub-bands with various security levels based on the user's requirement. At each level, a series of security mechanisms, including

authentication, confidentiality, and integrity, are used to protect data. The higher the security level labeled, the more the data protection provided. Only the subject with the proper security clearance can access the security-classified data. For example, a sub-band marked as RESTRICTED can be accessed by all the subjects in the group; and a sub-band marked as CONFIDENTIAL can only be accessed by the subjects classified as CONFIDENTIAL or higher; and so on. In general, lower-level subject can never access the object with greater security level. In addition, if needed, CB-MLDS may offer dynamic performance feedback on the security level chosen by users for a certain component, providing users with more resources to judge whether their security goals are satisfied.

Only user's data is protected is not enough, the security problem during data transmission in ad hoc networks is still a big concern. Routing is the heart of network infrastructure. So far there is no single routing protocol in ad hoc network adapt to the multilevel environment. Further, most ad hoc routing protocols take security for granted and assume that every node in the environment is trustworthy. Obviously, this assumption is not usually valid. Therefore, it's possible that malicious nodes take advantages of the trust relationship to paralyze an ad hoc network by inserting erroneous routing updates, replaying old routing information, changing routing updates, or advertising incorrect routing information. In order to protect routing process, Multi-Level On-demand Secure Ad hoc Routing (MOSAR), the other subsystem in MLDSS, is proposed.

MOSAR is designed to handle security classification during the routing process in ad hoc network. Every node in the group is initially assigned a certain security level,

basically based on their hierarchic ranks in the organization. In the multi-level secure routing, higher security-level nodes may be used by lower security-level nodes to relay the packets, but not the vise versa. In another words, if the security requirement on routing is RESTRICTED, then any node may be used to form a route. In such situation, the route with the shortest distance will be selected. If the security requirement on routing is SECRET, then only the nodes with security level equal or higher than SECRET can be employed to relay packets; and so forth. Therefore, a user has choice to send his packet via multiple routes with multiple security levels instead of only via the shortest route.

In this paper, the least read clearance level is denoted as RESTRICTED. The highest read clearance level is TOP SECRET. Similarly, the least route security level is referred to as RESTRICTED. The highest route security level is TOP SECRET. There are no limitations in how many levels may exist or how each is described; for practical purposes, this paper will work with groups of four levels of security. Here is the set of Read levels, RL= {RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET} and the set of Route levels TL= {RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET}. The user nodes are assigned a Read level from the set RL and a Route level from set TL. Each component has an associated Read level (one from the set RL) and a Route level (one from TL), assigned by the originator.

5.2 Content-Based Multi-Level Data Security (CB-MLDS)

While traditional data security system usually provides the same security services to a whole file, CB-MLDS provides multiple level security services to different components of a multimedia file, for the purpose of access control and the safety of storage. In other words, multiple classifications may exist simultaneously within a file, each of which is applied with corresponding security services. In this concept, entities are not just secure or insecure; they have varying degrees of sensitivity. Figure 5.2 illustrates the idea of CB-MLDS.

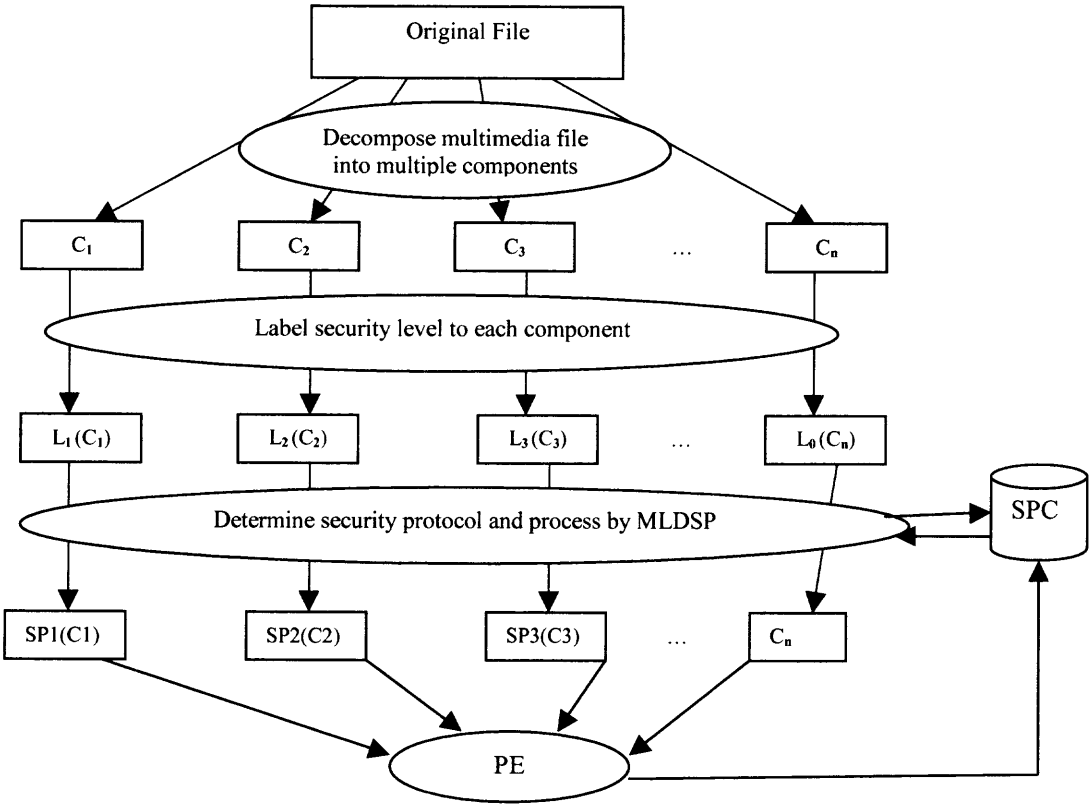

Figure 5.2 CB-MLDS Structure.

First, the original file is divided into a set of sub-bands. In this paper, wavelet-based decomposition is employed as the method of image decomposition. Several

wavelet filters and decomposition levels are supplied for user's options. After decomposition, each sub-band is associated with a proper Read level, chosen from the Read level set described earlier, based on the sensitivity of the content and the need-to-know requirement. A sub-band marked as RESTRICTED can be accessed and read by the members who have RESTRICTED or higher read clearance; and a sub-band labeled as TOP SECRET only can be accessed by members classified as TOP SECRET read level. By default, if Read level is not specified for a sub-band, then there is no security services required and it can be read by the members at any level. For each level, a security protocol is specially designed to provide security services. Each protocol implements some or all the security mechanisms such as authentication, integrity, confidentiality, and secrecy. In CB-MLDS, four security protocols, named SP1, SP2, SP3 and SP4 respectively are designed. The services provided by those protocols are shown in table 5.1.

Table 5.1 Security Protocol Assignment

Read Level	Security Protocol	Integrity	Authenticity	Confidentiality	Secrecy
RESTRICTED	SP1	Yes	No	No	No
CONFIDENTIAL	SP2	Yes	Yes	No	No
SECRET	SP3	Yes	Yes	Yes	No
TOP SECET	SP4	Yes	Yes	Yes	Yes

There is a trade-off between security and computation cost. Usually more complicated algorithms can provide higher security but with more computation cost. As long as his security goal is reached, user would rather choose the protocol that costs less resource, especially in the ad hoc network environment where both power and computation resources are limited. Security Performance Criterion (SPC) is a database

that provides dynamic feedbacks on the statistic performance of the security protocol selected by user. If the statistic result doesn't meet user's security goal, the user may switch to another security protocol at the same level.

After user determines security requirement for each sub-band, the sub-bands are processed by Multi-level Data Security Protocols (MLDSP), which actually process data using the corresponding security protocol for each sensitivity level. SP3 is used as an example to illustrate how the component marked as SECRET is processed and protected by the security protocol. As shown in Figure 5.3, a hash function is applied to the sub-band and the result is digitally signed by the user's private key. Then the signature is embedded into the component using watermarking technique. The position of the watermark is determined by the shared group key. The signed and watermarked component is encrypted with the group key again and the result is ready to distribute. As an important feature for component at SECRET level, user may hide secret message into the component.

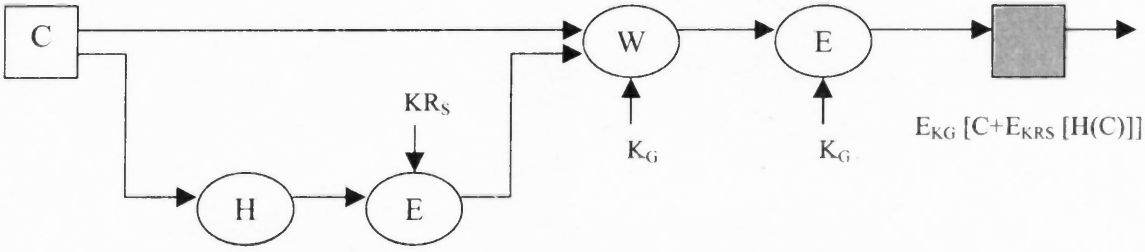

Figure 5.3 SP3 Procedure.

The output from MLDSP is sent to Performance Evaluation (PE) for attack tests. PE is an important part of the whole system. It consists of different attack protocols and a database that records the test results, illustrated by Figure 5.4. The result of each type attack is sent to SPC to update the statistic performance of the each security protocol.

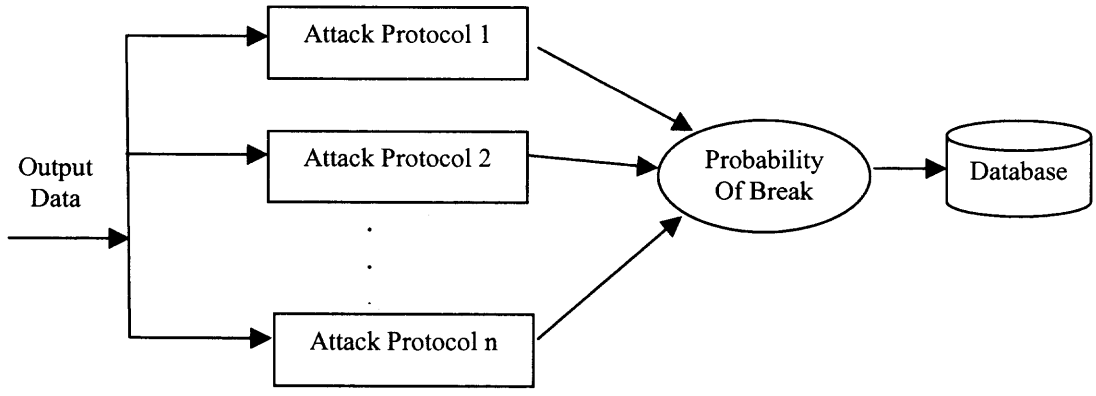

Figure 5.4 PE Scheme.

The recipient can only access the sub-band that is released to his security level, by providing correct secret group key. Also he may verify the authentication and check the integrity of the sub-band using sender's public key. This data processing procedure ensures that data is releasable only to those who have been authorized and that only a user who holds the correct secret key can access, derive and check the original data.

5.3 Mobile Multilevel On-demand Secure Ad hoc Routing (MOSAR)

5.3.1 Design Goals

We aim for a routing scheme that is able to handle the security classification of packets during the route discovery and route maintenance. The scheme should provide the network reasonable balances between security, performance and computation power efficiency. For above purposes, a new field called Route Security Requirement is added in the routing header as the indicator of security requirement. Therefore, routing is about to find the path from source to destination that all the nodes on which meet the security requirement. Besides, to protect routing packets against unauthorized disclosure,

modification or eavesdropping, the protocol offers different cryptographic mechanisms that are scalable to the computation resources at each Trust level for authentication and integrity check, and if necessary, packet secrecy. Our goal is to design a dependable and affordable routing protocol for ad hoc networks where the security requirements are different for different information to transmit, under different circumstances, or with different available resources.

5.3.2 Requirements

Our proposed routing protocol must provide the following security requirements:

REQ1: All the packets exchanged through the network must have a Route Security Requirement which indicates the security requirement of the requested route.

REQ2: All nodes participating in the protocol must have a Trust level. The node with a particular Trust level must only be allowed to transmit packets at that level or a level below it. This means that a node at TOP SECRET level is allowed to transmit packets that have any classifications, but a node at RESTRICTED level is only allowed to transmit packets labeled as RESTRICTED.

REQ3: The source originating a packet may be any one of the participating nodes but must be allowed to send a packet with Route Security Requirement only equal or below the Trust level of the source node. Therefore, only the nodes at the highest Trust level in the network may be allowed to possess the highest and lowest Route Security Requirement requests thereby enabling them to originate and transmit at any desired

level. This requirement can avoid bottle neck caused by nodes at low Trust levels over-classify their packets with high Route Security Requirement.

REQ4: Each level is supplied with corresponding-weight security services to assure the authenticity, integrity and secrecy of routing packets.

REQ5: If write down occurs, the protocol looks for indicators to show that an authorized node has approved it. The indicators usually include cryptographic authentication, like a digital signature. The protocol verifies the digital signature and checks the signer's identity against the list of users authorized to conduct downgrade.

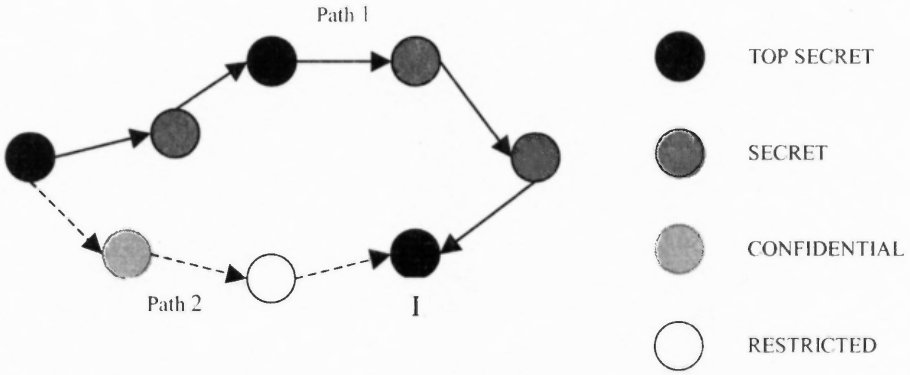

Figure 5.5 Example of Multilevel Secure Routing.

Figure 5.5 gives an example of multilevel secure routing. If source node S initiates a packet that is destined to node D and has route security requirement SECRET, this packet will be delivered following the path 1, since only the nodes whose Trust level are equal or higher than the Route Security Requirement are allowed to participate in route discovery. On the other hand, if the packet is classified as RESTRICTED, it will take path 2, because not only the nodes on path 2 meet the security requirement but also it has shorter distance. In this concept, packets are not just secure or insecure; they have varying degrees of sensitivity and are distributed via path with different security levels.

Hence, the scheme is able to provide communication that can handle the concept of security classifications.

5.3.3 Assumptions

For simplicity, we assume that the base protocol is an on-demand protocol similar to AODV or DSR, and all wireless links in the network are bidirectional, that is, if node A is able to transmit to some node B, then B is able to transmit to A. Since the resources of different ad hoc network nodes may vary greatly, it is reasonable to assume that the nodes at higher security levels have more computational resources. Each node keeps a list of identity of all the nodes in the ad hoc network. The identity table includes the assigned IP address, Trust level, public key. We assume that there is a secure way to update such information. Moreover, the nodes at higher Trust level would have keys relating to its own level and all the lower levels.

5.3.4 AODV

Since MOSAR is proposed basing on AODV, a brief review on this ad hoc routing protocol is given in the following section.

AODV [20] is a reactive protocol that determines routes solely on-demand. It is based on the distance vector technology. The hosts only know the next hop to every destination. When a source host wants to send packets to the destination and cannot get the routes from its routing table, it will broadcast a RREQ. The receivers may establish

the routes back to the source host through the paths that they get the RREQ. If the receiver has an active route to the destination, it will unicast a RREP back to the source. Otherwise, the RREQ will be re-broadcast further. If a reply is sent, all hosts along that path may record the route to the destination through this packet. Because there may exist multiple exclusive paths between two hosts, a mobile host can receive the same RREQ more than once. To prevent the same request from being broadcast repeatedly, every request is uniquely identified by a <Host ID, Broadcast ID> couple. Every host keeps a record for the RREQs that have been processed. The mobile hosts send out the Route Error (RERR) packets to their neighbors to report broken paths and activate the route re-discovery procedure.

To avoid routing loop and identify the freshness of the route, destination sequence number is introduced. The sequence number of a mobile host can only be updated by itself in monotonically increasing mode. A larger sequence number denotes a fresher route. The sequence number is carried in both RREQ and RREP. The sequence number in RREP must be larger than or equal to the one carried in corresponding RREQ to avoid the source host to adopt a stale path. When more than one path represented by different RREPs is available, the one with the largest destination sequence number is used. If several paths have the same sequence number, the shortest one is chosen. More details about AODV can be found in [20].

5.3.5 MOSAR Protocol

MOSAR is presented in 3 steps: first the mechanism that handles security classification is introduced; then the method for authenticating data in Route Request and Route Reply is explained; and finally the method that enables routing secrecy is brought in.

A. Packet Forwarding

According to REQ2 in section 5.3.2, each node participating in the protocol must be assigned a certain Trust level forehand. The assignment could be based on its hierarchic rank in the organization or the role it plays in the ad hoc network. When a source node wants to communicate with another node in the network, it constructs a message and labels the message with a Route Security Requirement, which indicates the security requirement on the requested route. The protocol then checks whether the Route Security Requirement satisfies the condition of REQ3 (see Section 5.3.2). If not, the node has to modify the classification of the message. Otherwise, the node initiates a Route Request (RREQ) packet, in which the Route Security Requirement is embedded as security metric, and then broadcasts it to its neighbors. The intermediate nodes receiving the RREQ first compare the value of Route Security Requirement in the RREQ with their own Trust levels. Based on REQ2 described in Section 5.3.2, only those intermediate nodes whose Trust level is equal or higher than the Route Security Requirement embedded in the RREQ packet are able to further process the RREQ, either forwarding the RREQ to their neighbors, or sending a Route Reply (RREP) back to the source node if a qualified route to the requested destination is available in their routing tables. When the RREQ reaches the destination, the destination sends a RREP back to the node from which it received the RREQ. The node forwards the RREP packet also establishes a

routing table entry for the destination, with the offered route security associated. When an intermediate node answers a RREQ query using cached information, the value of offered route security is compared to the security requirement in the RREQ packet. Only when the forward path can guarantee enough security is the cached path information sent back in the RREP.

If the Trust level of an intermediate node does not meet the requirement of the Route Security Requirement in the original RREQ, it has to drop the RREQ therefore it can not participate in the route discovery. In another word, nodes at higher Trust level may be used by nodes at lower Trust level to relay packets, but not the vise versa. For example, if the Route Security Requirement of a packet is RESTRITED, which means the lowest security requirement on a route, then any node in the ad hoc network has the qualification to participate in the route discovery. In such situation, the path with the shortest distance will be selected. If the Route Security Requirement is SECRET, then only the nodes at Trust level of SECRET and TOP SECRET are allowed to relay the packet.

The modification on the behavior of packet forwarding enables MOSAR to handle the concept of multilevel security; hence users are able to dispatch packets with various sensitivities via paths that possess corresponding security guarantees. In order to enforce the protocol working as designed and protect the network from certain vulnerabilities, the following mechanisms are also needed:

- Pre-loaded node identification table
- Control packet authentication
- Packet secrecy

It is the combination of above mechanisms provides the desired security and efficiency during route discovery and route maintenance. The details of some of the mechanisms are described next.

B. Pre-loaded Node Identification Table

Besides provided with a public/private key pair and a secret group key, every node that participates in the protocol is pre-loaded an identity table which could be used when authentication is needed. In order to acquire the identity table, nodes need to log in an identity manager, which is assumed to be secure and uncompromisable. The identity table provides information about the other peer nodes in the network. Each entry of the table describes the identity of a specific node. It binds the following information together with the node: IP address, security clearance level, public key, valid time period. The trusted identity manager has to reflect the current bindings of nodes in the ad hoc network, and nodes need to contact the identity manager when the service is available to keep the freshness and correctness of the identity table. Appropriate mechanisms should be applied to guarantee the secure communications between nodes and the security manager. However, it is not the focus of this paper, for more detailed discussion on this topic, please see the related references.

C. Authentication

MOSAR may employ the following properties to secure routing packets: the destination node can authenticate the RREQ issued by source node; the intermediate nodes forwarding the RREQ/RREP can authenticate each other.

Authentication can be provided with symmetric cryptographic techniques such as message authentication code (MAC), and asymmetric cryptographic techniques such as

digital signature. MAC relies on a secret key shared between the two communicating parties. While MAC is an efficient way for authentication, it brings the problem of key management, which is complicated, and is always subject to attacks by adversaries. On the other hand, digital signature is a straightforward method that uses public/private key pair to provide not only source authentication but also non-repudiation of origin. The disadvantage is that the computation cost on resource-constrained nodes is expensive, which is several orders of magnitude higher than a MAC. For example, Brown et al analyze the computation time of digital signature algorithms on various platforms [10]; on a Palm Pilot or RIM pager, a 512-bit RSA [21] signature generation takes 2.4–5.8 seconds and signature verification takes 0.1–0.6 seconds, depending on the public exponent.

The resources of different ad hoc network nodes may vary greatly. In the environment where multilevel security is needed, it is reasonable to assume that the nodes classified at higher Trust levels have more computational resources and energy than the nodes at lower Trust levels. In this work, a hybrid authentication protocol, which is based on the combination of MAC and digital signature, is used to provide a balance between security, performance and resource.

For routing packets with high security requirement such as TOP SECRET and SECRET, security is the most important concern. Besides, nodes initiate and forward such packets have enough computation resource. In this circumstance, digital signatures are used for hop by hop authentication. The difference between our scheme and ARAN is that, instead of appending a digital certificate in the RREQ and RREP, the IP address of the forwarding node is appended as the proof of its identity. Based on the IP address,

other nodes in the network can use the pre-loaded identity table to obtain the required public key and verify its Trust level.

The detailed process is illustrated by the following example. When a node S wants to communicate with another node D in the network, it generates a route request (RREQ) which contains the regular fields in AODV such as route request identification number, source address, source sequence number, destination address, destination sequence number, timestamp, and one new additional field: route security requirement. The initiator S signs the RREQ with its private key and broadcasts to its neighbours. Each node that is qualified to forward this RREQ checks the signature, using the corresponding public key stored in the identity table. Node *C* checks node *B*'s signature on the outer message. *C* then verifies the signature of initiator S on the RREQ. If the signatures are valid, the forwarding node removes the last forwarder's signature and signs the original RREQ with its own private key. The node then broadcasts the RREQ.

$$S: \quad \mathrm{sig_S} = (\mathrm{RREQ, ID, IP_S, SEQ_S, IP_D, OLDSEQ_D, T_S, RREQ\_SEC})\mathrm{K_{S_V}}$$
$$S \rightarrow *: \quad \{\mathrm{RREQ, ID, IP_S, SEQ_S, IP_D, OLDSEQ_D, T_S, RREQ\_SEC}\}, \mathrm{sig_S}$$
$$A \rightarrow *: \quad \{\mathrm{RREQ, ID, IP_S, SEQ_S, IP_D, OLDSEQ_D, T_S, RREQ\_SEC}\}, (\mathrm{sig_S})\mathrm{K_{A_V}}, \mathrm{IP_A}$$
$$B \rightarrow *: \quad \{\mathrm{RREQ, ID, IP_S, SEQ_S, IP_D, OLDSEQ_D, T_S, RREQ\_SEC}\}, (\mathrm{sig_S})\mathrm{K_{B_V}}, \mathrm{IP_B}$$
$$C \rightarrow *: \quad \{\mathrm{RREQ, ID, IP_S, SEQ_S, IP_D, OLDSEQ_D, T_S, RREQ\_SEC}\}, (\mathrm{sig_S})\mathrm{K_{C_V}}, \mathrm{IP_C}$$
$$D: \quad \mathrm{sig_D} = (\mathrm{RREP, IP_D, SEQ_D, IP_S, T_D, RREQ\_SEC})\mathrm{K_{D_V}}$$
$$D \rightarrow C: \quad \{\mathrm{RREP, IP_D, SEQ_D, IP_S, T_D, RREQ\_SEC}\}, \mathrm{sig_D}$$
$$C \rightarrow B: \quad \{\mathrm{RREP, IP_D, SEQ_D, IP_S, T_D, RREQ\_SEC}\}, (\mathrm{sig_D})\mathrm{K_{C_V}}, \mathrm{IP_C}$$
$$B \rightarrow A: \quad \{\mathrm{RREP, IP_D, SEQ_D, IP_S, T_D, RREQ\_SEC}\}, (\mathrm{sig_D})\mathrm{K_{B_V}}, \mathrm{IP_B}$$
$$A \rightarrow S: \quad \{\mathrm{RREP, IP_D, SEQ_D, IP_S, T_D, RREQ\_SEC}\}, (\mathrm{sig_D})\mathrm{K_{A_V}}, \mathrm{IP_A}$$

When the RREQ from a route discovery reaches the destination, the destination signs a RREP and sends it to the node from which it received the RREQ. In the example,

the destination *D* returns a signed RREP to the previous hop *C*. The RREP is forwarded in much the same way as the RREQ, except that each node unicasts the RREP to the node from which it received the RREQ. In particular, each node receiving a RREP checks the signature or signatures. In our example, node B first checks the signature on the outer message, then it verifies the signature on the RREQ using node D's public key. If the signatures are valid, the forwarding node removes the last forwarder's signature, signs the original RREP. It then unicasts the RREP back to the node from which it received the associated RREQ. In the example, node B removes node C's signature, signs the resulting RREP and then unicasts the resulting RREP to *A*, from which it had previously heard the RREQ.

In above authentication scheme, more than one digital signature is used to authenticate routing packets from source, destination and intermediate nodes. This method prevents certain impersonation attacks. But it is vulnerable to Denial of Service (DoS) [2] attacks based on flooding the network with bogus control packets for which signature verifications are required. Therefore, this method requires nodes have enough resource to verify signatures at line speed.

A routing packet associated with lower route security requirement can be initiated and forwarded by nodes which are not necessarily equipped with high computation power. In such case, using asymmetric cryptographic mechanisms to sign the packets at each intermediate node could be too expensive. On the other hand, the computation complexity and power consumption of symmetric key cryptographic operations are negligible when compared with public key schemes. Therefore, for the routing packets that security is important but not critical, an intermediate node only attaches a Message

Authentication Code (MAC), which is calculated by applying a hash function with a group key. Other intermediate nodes may use the MAC to check the integrity of the message and to verify the qualification of the node who forwarded the message. While this group key approach is efficient both in terms of computation and communication overhead, it just mitigates outside attacks and does not protect against compromise of a single node. Therefore, digital signature is still needed at the source and destination node, when they send RREQ and RREP respectively. As showed in the following example, the source node S first broadcasts the RREQ packet with its signature. If node A satisfies the security requirement in RREQ (node A's Trust level >= RREQ_SEC), it calculates a MAC, using the shared group key at the level of RREQ_SEC, over the RREQ packet, the signature and A's IP address. Node A then rebroadcasts the RREQ along with the authentication tag. When node B receives the message from node A, it verifies A's identity against the identity table, and then check the integrity of the message. When the RREQ reaches the destination, node D verifies the digital signature of S, signs a RREP, and unicasts back to the node from which the RREQ was received. The authentication process of RREP at intermediate nodes is similar as the one of RREQ.

S: $\text{sig}_S = (\text{RREQ}, \text{ID}, \text{IP}_S, \text{SEQ}_S, \text{IP}_D, \text{OLDSEQ}_D, \text{T}_S, \text{RREQ\_SEC})\text{K}_{S_V}$

$S \rightarrow *$: $\{\text{RREQ}, \text{ID}, \text{IP}_S, \text{SEQ}_S, \text{IP}_D, \text{OLDSEQ}_D, \text{T}_S, \text{RREQ\_SEC}\}, \text{sig}_S$

A: $\text{M}_A = \text{MAC}_{K_G}(\text{RREQ}, \text{ID}, \text{IP}_S, \text{SEQ}_S, \text{IP}_D, \text{OLDSEQ}_D, \text{T}_S, \text{RREQ\_SEC}, \text{sig}_S, \text{IP}_A)$

$A \rightarrow *$: $\{\text{RREQ}, \text{ID}, \text{IP}_S, \text{SEQ}_S, \text{IP}_D, \text{OLDSEQ}_D, \text{T}_S, \text{RREQ\_SEC}\}, \text{sig}_S, \text{M}_A, \text{IP}_A$

B: $\text{M}_B = \text{MAC}_{K_G}(\text{RREQ}, \text{ID}, \text{IP}_S, \text{SEQ}_S, \text{IP}_D, \text{OLDSEQ}_D, \text{T}_S, \text{RREQ\_SEC}, \text{sig}_S, \text{IP}_B)$

$B \rightarrow *$: $\{\text{RREQ}, \text{ID}, \text{IP}_S, \text{SEQ}_S, \text{IP}_D, \text{OLDSEQ}_D, \text{T}_S, \text{RREQ\_SEC}\}, \text{sig}_S, \text{M}_B, \text{IP}_B$

C: $\text{M}_C = \text{MAC}_{K_G}(\text{RREQ}, \text{ID}, \text{IP}_S, \text{SEQ}_S, \text{IP}_D, \text{OLDSEQ}_D, \text{T}_S, \text{RREQ\_SEC}, \text{sig}_S, \text{IP}_C)$

$C \rightarrow *$: $\{\text{RREQ}, \text{ID}, \text{IP}_S, \text{SEQ}_S, \text{IP}_D, \text{OLDSEQ}_D, \text{T}_S, \text{RREQ\_SEC}\}, \text{sig}_S, \text{M}_C, \text{IP}_C$

D: $\text{sig}_D = (\text{RREP}, \text{IP}_D, \text{SEQ}_D, \text{IP}_S, \text{T}_D, \text{RREQ\_SEC})\text{K}_{D_V}$

$D \rightarrow C$: $\{\text{RREP}, \text{IP}_D, \text{SEQ}_D, \text{IP}_S, \text{T}_D, \text{RREQ\_SEC}\}, \text{sig}_D$

D. Routing Confidentiality

For messages that are classified with high security requirement, for example, TOP SECRET, the exchange of routing packets itself could release some sensitive information, such as network topology. Hence, it is necessary to keep the routing packets with high security requirement confidential, by encrypting certain fields of RREQ and RREP with the group secret key. Since the group key is shared only within the group members, nodes at lower Trust levels can not decrypt the routing messages thus they even do not know the occurrence of packet exchange at high security level.

5.3.6 Prevention and Protection

MOSAR is equipped with special protection features that are different from other proposed ad hoc secure routing protocols:

- Instead of using shortest distance as the routing metric, MOSAR embeds route security requirement in control packets. Routing is about to find a trusted route that meets the security requirement. Once a secure route is established, data forwarding over that route is a simple matter. Thus black hole and worm-hole attacks are effectively prevented.

- The hierarchy structure of MOSAR is a desirable property for routing protocols because it helps to limit failures to smaller areas in a network. As it also limits the number of routing messages in comparison with flat routing, it may also limit the vulnerability against denial-of-service attacks and sleep deprivation attacks based on excessive route requests.

- MOSAR increases route robustness by providing more route choices through multilevel route discovery and maintenance. For example, if a route at certain security level is broken, a source node can still communicate with the destination node using route at other security levels.

- In MOSAR, user can classify packets with varying security requirement and apply varying-weight protection methods, which in turn minimize the delays or burdens on the system that may occur from heavy-weight cryptographic methods.

- In MOSAR, participants accept only packets that have been processed with a node whose identity is listed in the pre-loaded identity table and also meets the security requirement embedded in the packets. Moreover, the packets are signed either with a node's private key or secret group key. Therefore, an unauthorized node can not participate in the routing process since its identity is not included in the identity table and it does not have a valid key to sign the routing packets.

- Since only the source node can sign with its own private key, nodes cannot spoof other nodes in route instantiation. Similarly, reply packets are signed by the destination node, ensuring that only the destination can respond to route discovery. This prevents impersonation attacks where either the source or the destination node is spoofed.

- Messages at a certain security level can be fabricated only by nodes at the same or higher Trust levels. In that case, MOSAR only partially prevents fabrication of routing messages, but it does reduce the chance that routing messages at high security level are fabricated. Further, it ensures non-repudiation for high security level messages by signing with a node's private key.

- MOSAR specifies that all fields of RREQ and RREP packets remain unchanged between source and destination. Since both packet types are signed by the initiating node, any alterations in transit would be detected by intermediary nodes along the path, and the altered packet would be subsequently discarded. Thus, modification attacks are prevented.

- Replay attacks are prevented by including a timestamp with routing messages.

- By encrypting certain fields of RREQ and RREP at higher security level, read-up violation can be prevented from the malicious nodes with lower Trust level, who can not interpret the packets without higher-level group key.

5.4 Summary

There are two ways to provide confidentiality to a storage or transmission application. First, confidentiality is based on mechanisms provided by the underlying computational infrastructure. The advantage is complete transparency, i.e. the user or a specific application does not have to take care about confidentiality. The obvious disadvantage is that confidentiality is provided for all applications, no matter if required or not, and that it is not possible to exploit specific properties of certain applications. For example, consider a real-time image/video distribution system. If the connections among the components are based on TCT/IP internet-connections, which are not confidential by itself, confidentiality can be provided by creating a Virtual Private Network (VPN) using IPSec, which extends the IP protocol by adding confidentiality and integrity features. In this case, the entire visual data is encrypted for each transmission that puts a severe load on the encryption system. The second possibility is to provide confidentiality on the application layer. Here, only applications and services are secured which have a demand for confidentiality. The disadvantage is that each application needs to take care for confidentiality by its own; the advantage is that specific properties of certain applications may be exploited to create more efficient encryption schemes or that encryption is omitted if not required.

The content-based multi-level data security subsystem is therefore, classified into the second category; whereas the multi-level secure routing subsystem belongs to the first category.

CHAPTER 6

EXPERIMENT RESULTS AND DISCUSSION

6.1 Experiment On CB-MLDS

6.1.1 Experiment Setup

In the experiment, wavelet is employed as the image decomposition method. The reason we choose wavelet over Fourier techniques is that the data sets without obviously periodic components cannot be processed well using Fourier techniques. Wavelets allow complex filters to be constructed for this kind of data which can remove or enhance selected parts of the signal. There is a growing body of literature on wavelet techniques for noise reduction. Wavelets have been used for data compression. For example, the United States FBI compresses their fingerprint database using wavelets. Lifting scheme wavelets also form the basis of the emerging JPEG 2000 image compression standard. Wavelet techniques have also been used in a variety of statistical applications, including signal variance estimation, frequency analysis and kernel regression.

In the experiment, the original data being processed is a gray-level image consists of 256 by 256 pixels; each pixel is expressed by 8 bits. Wavelet "haar" is employed to do single-level discrete 2-D wavelet transform. Four sub-bands are obtained after wavelet decomposition.

Usually LL sub-band retains the most important information for human eyes. For the security of an image, this sub-band is classified as higher security level and is processed with more complicated security protocol. On the other side, the information in some sub-bands is hardly recognized by human eyes, we choose not to process them as a trade-off between security and computational efficiency. Table 6.1 lists the sub-bands

that need to be processed for each sensitivity level with corresponding security protocols (refer to table 5.1).

Table 6.1 Processing Detail

Sub-band Sensitivity	SB1	SB2	SB3	SB4
TOP SECRET	SP4	-	-	-
SECRET	-	SP3	-	-
CONFIDENTIAL	-	-	SP2	-
RESTRICTED	-	-	-	SP1

Usually images are the data type that requires enormous storage capacity or transmission bandwidth due to the large amount of data involved. In order to provide reasonable execution performance for encrypting such large amounts of data, only symmetric encryption can be used. In the experiment, AES (Advanced Encryption Standard), a recent symmetric block cipher which is going to replace DES (Data Encryption Standard) in all applications where confidentiality is really the aim, is applied as the encryption method in our security protocols for all sensitivity levels. AES operates on 128-bit blocks of data and uses 128, 196, or 256 bit keys. The length of the key determines the degree of security. Therefore, 256 bit key is applied in the highest-level security protocol, namely, SP4, 196 bit key in SP3 and 128 bit key in SP2 respectively. Moreover, SHA1 (Secure Hash Algorithm) is used for the purpose of integrity check in the security protocols at all levels. RSA, a public key technique, is used in SP2, SP3 and SP4 for signature generation as the method of authentication.

6.1.2 Experiment Results

Figure 6.1 displays the test images used in our experiment; Figure 6.2 shows the result of the original image after single-level wavelet decomposition.

Figure 6.1 Original Image.

Figure 6.2 Sub-bands.

Figure 6.3 shows the result that the entire image was processed with SP3. The processing time was 30.78 seconds. Figure 6.4 demonstrates the results that each sub-band being processed by the corresponding security protocol, as shown in Table 6.1. The processing time is 13.98 seconds. Obviously, the processing time in the latter case is more than 2 times shorter than the one in the first case.

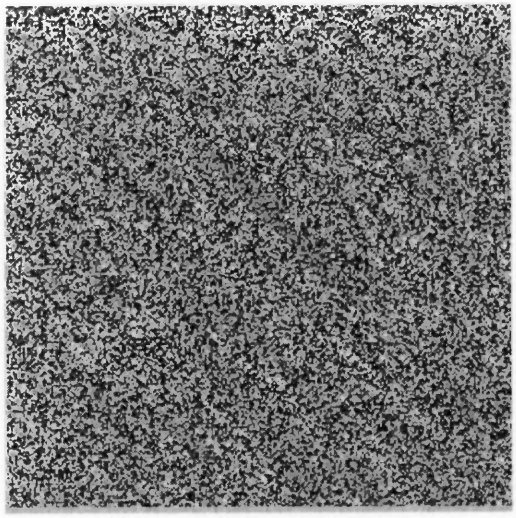

Figure 6.3 Entire Image Processed By SP3.

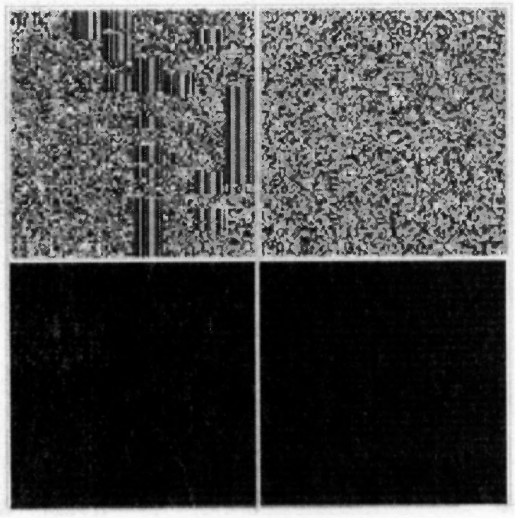

Figure 6.4 Each Sub-band Processed By Different Security Protocol.

It is noticed that CB-MLDS provides flexibility and adaptability for user. A user is able to tune the security level for his data to meet the security requirement. Therefore, a balance can be reached between the processing speed and security.

6.2 Simulations On MOSAR

6.2.1 Simulation Set Up

The purpose of the simulation is to study the effect of security levels involved in routing to the performance of an ad hoc network. The implementation of MOSAR is based on AODV model in Opnet [22]. A new field is added to represent the route security requirement in route request and route reply packets; the size of each routing packet is also increased to accommodate digital signature or MAC for the purpose of authentication. In MOSAR, 16 byte signature/MAC is used. These values are reasonable to prevent compromise during the short time nodes spend in the routing process.

In more detail, a new attribute, "Security Level", is added to each node in the network, representing the pre-assigned Route clearance of that node. RREQ packets have an additional field called RREQ_SEC_REQUIREMENT that indicates the required security for the route the sender wishes to discover. This field is set by the sender and validated by the protocol to make sure that the set up does not violate the pre-defined authority rule, which regulates that node with a certain Route clearance can not send a RREQ in which the value of RREQ_SEC_REQUIREMENT is greater than its own Route clearance. Once a valid RREQ_SEC_REQUIREMENT is set up, it does not change during the route discovery. When an intermediate node receives a RREQ packet, the protocol first checks if the Route clearance of this node meets the security requirement indicated in the packet. If the node is qualified to participate in the routing, the proposed protocol behaves like the regular AODV and the RREQ packet is forwarded. Otherwise, the RREQ is dropped by the intermediate node.

The arrival of a RREQ packet at the destination indicates the existence of a path from the sender to the receiver that satisfies the security requirement specified by the sender. The destination sends a RREP packet as in the normal AODV, but with an additional field which is RREP_SEC_OFFERED. The value of the RREQ_SEC_REQUIREMENT in RREQ is copied to the field of RREP_SEC_OFFERED in RREP packet. While the RREP is sent back along the reverse of the discovered path, the routing table of each intermediate node on the path is updated. In each route entry of a routing table, a new field called RT_SEC_LEVEL_SUPPORT is added. When a qualified intermediate node answers a RREQ using cached information, this value is compared to the security requirement in the RREQ packet. Only when the

forwarded path can satisfy the required security, the cached path information is sent back in the RREP.

In the simulations, 50 nodes move around in 1500m by 300m region. Node's transmission range is 250 meters. Nodes move according to the random waypoint mobility model [23]. Each node is initially placed at a random location and pauses for a period of time called the pause time; it then chooses a new location at random and moves there with a velocity randomly chosen uniformly between 0 and the maximum speed. When it arrives, it repeats the process of pausing and then selecting a new destination to which to move. There are 20 source-destination pairs, each sending a Constant Bit Rate (CBR) flow of 4 data packets per second. Each data packet is 512 bytes in size. In order to compare the performance of MOSAR and AODV, both protocols are run under identical mobility and traffic pattern.

Four scenarios were simulated:

- In the first scenario, all 50 nodes have the same Trust level and all traffic flows have the same Route Security Requirement. Routing follows the normal AODV behaviors.

- In the second scenario, 50 nodes are classified into 2 Trust levels: 20 nodes are at CONFIDENTIAL and 30 nodes are RESTRICTED level, respectively. 50% traffic flow have Route Security Requirement of CONFIDENTIAL and the rest of traffic flows RESTRICTED.

- In the third scenario, 50 nodes are classified into 3 Trust levels: 10, 10 and 30 nodes are at SECRET, CONFIDENTIAL and RESTRICTED, respectively. First the situation where the traffic flows follow the pattern of 30% SECRET, 25% CONFIDENTIAL and 45% RESTRICTED, respectively was simulated.

- In the fourth scenario, a routing failure in MOSAR was simulated. 8, 12 and 30 nodes are at SECRET, CONFIDENTIAL and RESTRICTED, respectively. The traffic flows follow the pattern of 30% SECRET, 25% CONFIDENTIAL and 45% RESTRICTED, respectively. The 8 nodes at SECRET level are purposely arranged in a topology that some of the source/destination pairs are out of the relay range.

6.2.2 Simulation Results

In the simulation, the effect of number of involved security levels in a network was studied; the effect of node pause time to the network performance in each scenario was demonstrated; the effect of moving speed as well as transmission range was analyzed. The network performance for MOSAR is measured along three metrics:

- Routing packet overhead: This is the number of control packet overhead. The transmission at each hop along the route was counted as one transmission in the calculation of this metric.
- Average route discovery time: This is the average time needed between the sending of a route request packet by a source node for discovering a route to a destination and the receipt of the first corresponding route reply.
- Packet Delivered: The total number of CBR packets received out of the total number of CBR packets originated.

Figure 6.5 to Figure 6.9 show the results where scenario 1, 2, 3 are simulated with maximum moving speed of 20meters per second and the node pause time is 40 seconds. Figure 6.5 and Figure 6.6 show that with more levels of Route Security Requirement involved in the ad hoc network, less routing packet overhead were produced. This is because that only the intermediary nodes that meet the Route Security Requirement in RREQ and RREP can forward the packets. Figure 6.7 demonstrates that route discovery time increased with more security levels involved. The explanation is that the routing packets with higher Route Security Requirement can not be relayed by nodes at lower Trust levels, therefore for a node launches a RREQ with higher Route Security Requirement, the probability of its receiving replies quickly from nearby nodes is low due to the decreased connectivity of all the nodes resulting in increased route discovery latency. This also can be verified in Figure 6.8, which shows the number of hops per route was reduced with more security level involved.

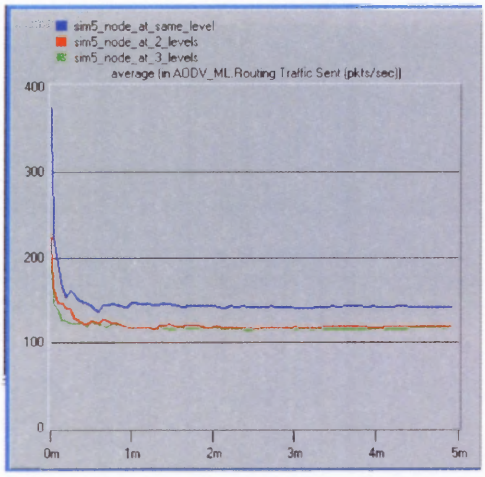

Figure 6.5 Routing Traffic Sent.

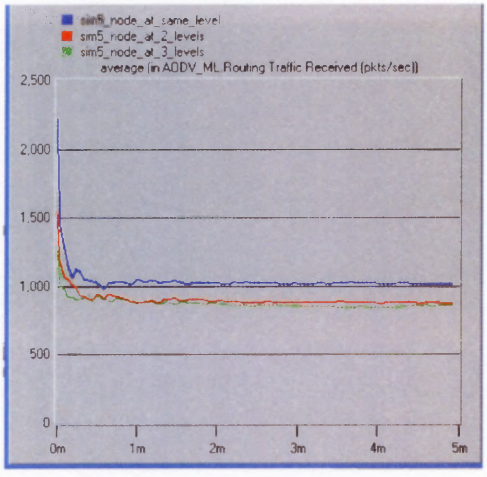

Figure 6.6 Routing Traffic Received.

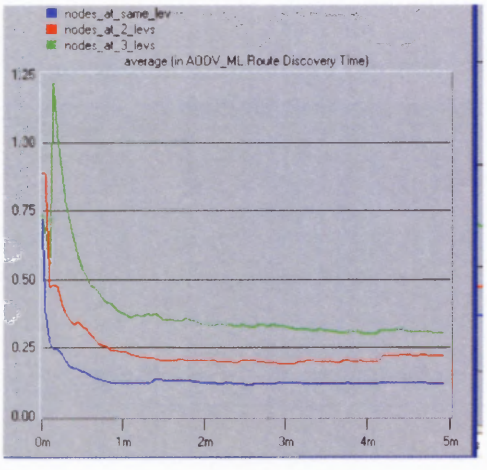

Figure 6.7 Route Discovery Time.

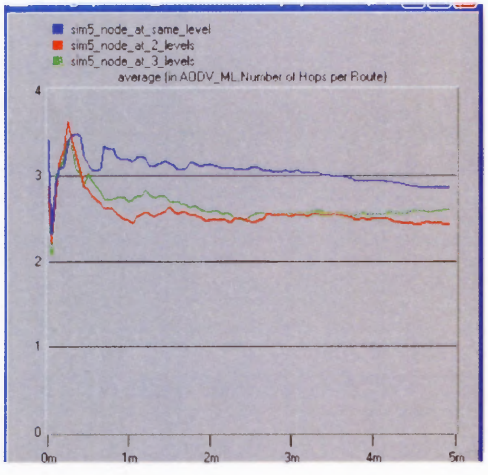

Figure 6.8 Number of Hops per Route.

Figure 6.9 illustrates the CBR packets delivered successfully to the destination nodes. It is noticed that the involvement of more security levels does not have dramatically effect on the overall throughput, which falls in the range from 94% to 96%. The throughput in the scenario of two security levels involved is about 1% higher than the one that a single security level is involved.

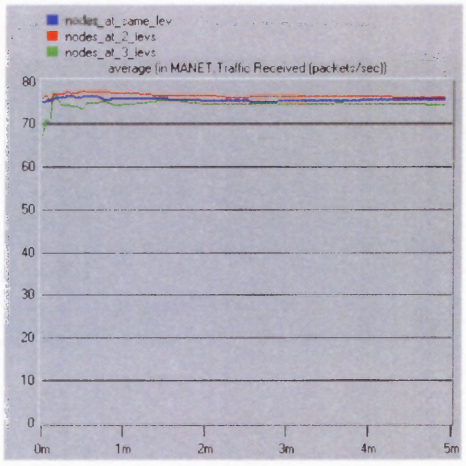

Figure 6.9 Traffic Received.

Figure 6.10 and 6.11 display the effect of various pause time to the performance in scenario 1, 2, 3. While the route discovery time has little change in the network where only a single security level is involved, it reaches the smallest value when the pause time is 40 seconds in the networks where two or more security levels are involved.

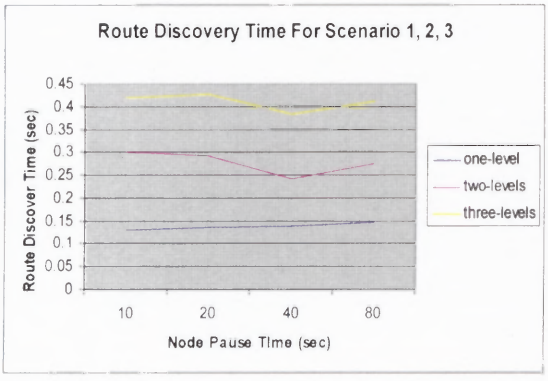

Figure 6.10 Route Discovery Time.

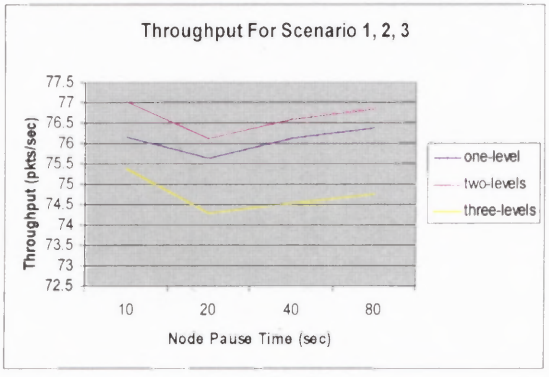

Figure 6.11 Throughput.

Figures 6.12 to 6.15 show the results of scenario 1, 2, 3 with node moving speed of 5 meters per seconds. Comparing with the results obtained from scenario 1, 2, 3 with moving speed of 20 meters per seconds, we observe that the routing traffic sent in the three scenarios did not change with the change of speed (Figure 6.12), but the routing traffic received is about 12% more in scenario 1 (where only a single security level is

involved) with the decrease of moving speed while it did not change in the scenarios with more security levels involved (Figure 6.13). On the other side, Figure 14 shows that the route discovery time did not change in scenario 1 while it decreased in scenario 2 and scenario 3 with the reduce of moving speed. In addition, the throughput still fell in the same range for all scenarios.

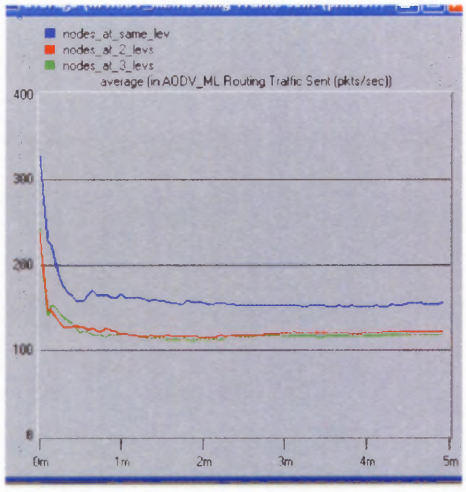

Figure 6.12 Routing Traffic Sent.

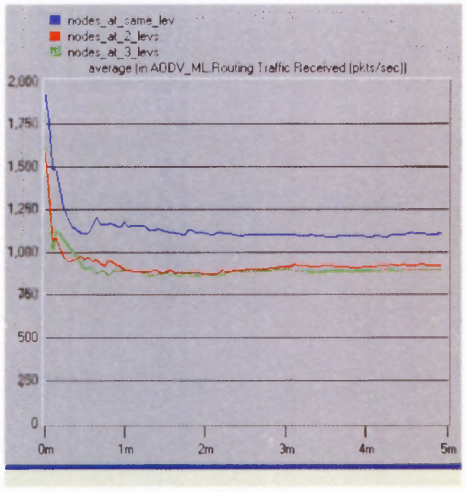

Figure 6.13 Routing Traffic Received.

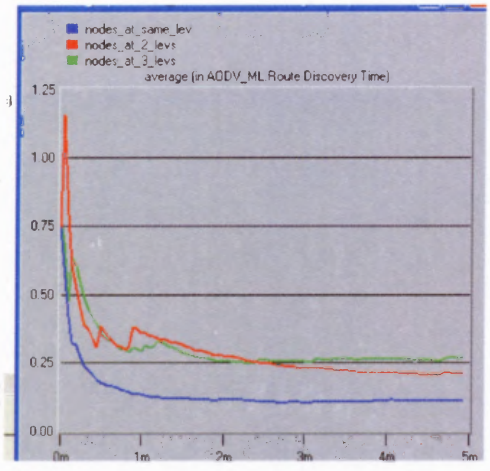

Figure 6.14 Route Discovery Time.

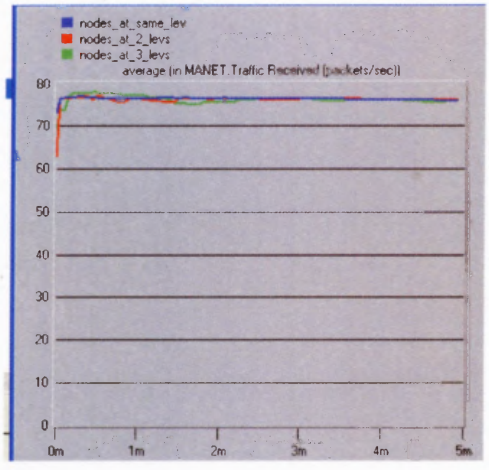

Figure 6.15 Traffic Received.

Figure 16 illustrates the results of scenario 1, 2, 4 with maximum node moving speed of 20 meters per second and pause time 40 seconds. As described earlier, the 8 nodes at SECRET level in scenario 4 were purposely arranged in a topology that some of the source/destination pairs are out of the relay range, therefore routing failure occurred. The throughput in scenario 4 is about 55 packets per second, which is much lower than the one in the other two scenarios. The explanation is that some packets with Route Security Level of SECRET could not be delivered, since no route was discovered between the source and destination pairs. This drawback can be avoided and the performance can be improved by increasing the node transmission range. In the early sections, we assumed that the nodes with higher Trust level possess more resources, including both energy resources and computational resources. Thus the nodes at higher Trust level are able to transmit with higher power and longer distance. Figure 6.17 shows that when the transmission range of nodes at SECRET level was increased to 500 meters from 250 meters, the throughput was also dramatically increased. This is easy to understand because the routes were unavailable before can be discovered with longer transmission range hence longer relay distance.

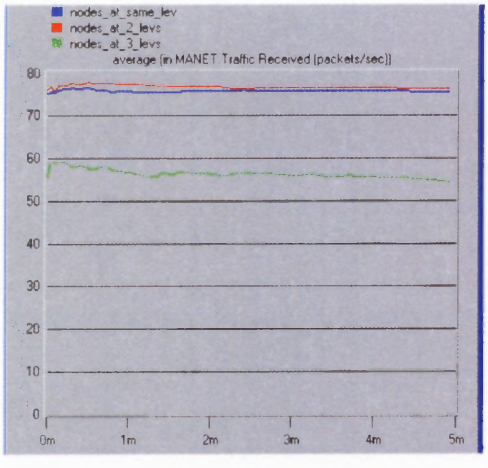

Figure 6.16 Traffic Received.

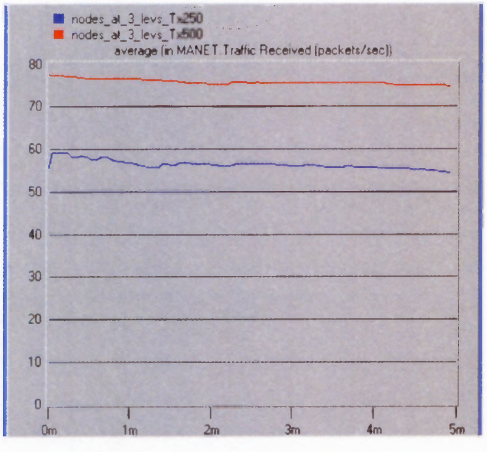

Figure 6.17 Traffic Received.

The effect of transmission range is more obvious in the scenarios that more than one security levels involved. Figure 6.18 shows the results that the transmission range for all nodes in scenario 1, 2 and 3 is 500 is increased to 500 meters. We observe that scenario 3 produced the least routing traffic and has the shortest route discovery time in all scenarios.

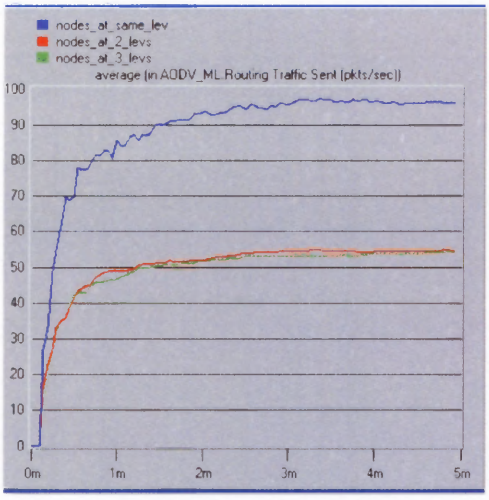

Figure 6.18 Routing Traffic Sent.

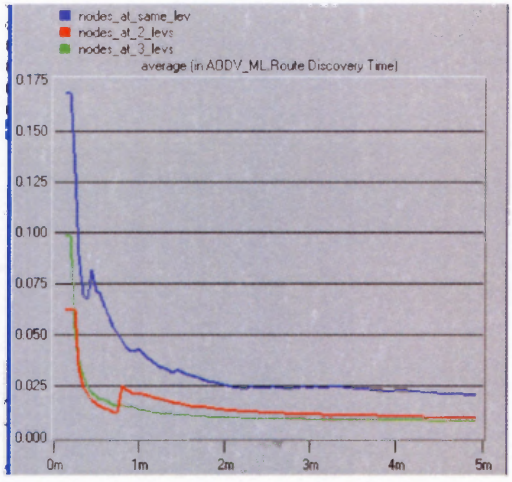

Figure 6.19 Route Discovery Time.

From above results, we can conclude that MOSAR functions well in handling classification and it can perform better than the regular AODV protocol.

6.2.3 Quantitative Security Assessment

Conventionally, the evaluations on the protection measures of ad-hoc secure routing protocols were conducted on the qualitative basis, as described in section 5.3.6. For the malicious activities that critically increase the risk of ad hoc networks, there is no one assessment model yet that considers a unified scheme of vulnerabilities, threats, and countermeasures. A quantitative risk assessment provides results in numbers that

management can understand, whereas a qualitative approach makes it difficult to trace generalized results. In this dissertation, a quantitative assessment model [24] is applied as an addition to evaluate MOSAR.

6.2.3.1 Overview of Quantitative Assessment Model. Mehmet proposed a quantitative risk assessment model in [24]. Three ingredients, vulnerability, threat, and countermeasure (CM), are involved in the model and their probabilities are used as input to calculate the residual risk of a system. A vulnerability is a weakness in any information system or system security protocol that an attacker could exploit. Threat is any circumstance or event with the potential to adversely impact a system, through unauthorized access, destruction, disclosure, modification of data, or denial of service. A CM is an action or technique that reduces risk to an information system. Consequently, the residual risk is the portion of risk remaining after a CM is applied. Residual risk can be zero if a perfect CM exists. A system may totally have n vulnerabilities that could be exploited by an attacker. If the probability of the *ith* vulnerability is V_i, then $\sum_n V_i = 1$.

There may have several threats to be employed to take advantage of a specific vulnerability. If vulnerability V_i has m threats, and T_j is the probability of the *jth* threat of vulnerability V_i, then $\sum_m T_j = 1$. Each threat has a countermeasure (CM) that ranges between 0 and 1 whose complement gives the lack of CM (LCM). An example of how the residual risk of a system is calculated is illustrated in Figure 6.20 [24].

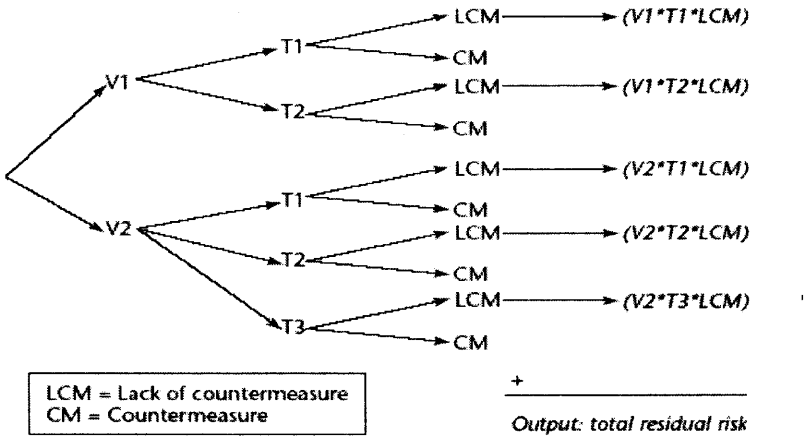

Figure 6.20 Quantitative Risk Assessment Model [24].

6.2.3.2 Quantitative Analysis on MOSAR. In this section, the quantitative analysis is conducted on MOSAR using the model introduced earlier. Firstly the vulnerabilities and the threats on AODV routing protocol are summarized, and the corresponding countermeasures provided by MOSAR are listed. Next, the probability for each element is assigned. To simplify, we assume that all vulnerabilities have the same probability to be exploited by an attack. That is, if there are n vulnerabilities in a system, the probability that each vulnerability could be exploited is 1/n. The same idea applies on the threat probability assignment. Also, we assume that if a threat is completely prevented by a countermeasure, the probability of lack of countermeasure is 0; if a threat is partially prevented by a countermeasure, the probability of countermeasure is 0.5 and the probability of lack of countermeasure is 1-0.5=0.5; if there is no any countermeasure to a threat, then the probability of lack of countermeasure is 1 (see Table 6.2). In practice, the probability input could vary, depending on the actual environment.

According to the example showed in Figure 6.20, the residue risk is calculated after applying MOSAR as the routing protocol for an ad hoc network that has vulnerability and threat parameters defined as above.

$$Total\,\mathrm{Re}sidueRisk = v1 * t1 * LCM_{11} + v2 * t2 * LCM_{22} + v7 * t1 * LCM_{71}$$
$$= \frac{1}{7} * \frac{1}{2} * \frac{1}{2} + \frac{1}{7} * \frac{1}{2} * \frac{1}{2} + \frac{1}{7} * 1 * \frac{1}{2} = \frac{1}{7}$$

Table 6.2 Vulnerabilities, Threats and Countermeasures

Vulnerability	Threat	Countermeasure (CM) & Lack of Countermeasure (LCM)
		MOSAR
Unnecessary route request v1=1/7	Rushing attack t1=1/2	CM_{11}=1/2 LCM_{11}=1/2
	Black hole t2=1/2	CM_{12}=1 LCM_{12}=0
Malicious routing query flooding to non-exist nodes v2=1/7	Routing table overflow t1=1/2	CM_{21}=1 LCM_{21}=0
	Sleep deprivation t2=1/2	CM_{22}=1/2 LCM_{22}=1/2
False destination sequence v3=1/7	Black hole with spoofing t1=1	CM_{31}=1 LCM_{31}=0
Fabrication of error messages v4=1/7	Black hole t1=1/2	CM_{41}=1 LCM_{41}=0
	Spoofing t2=1/2	CM_{42}=1 LCM_{42}=0
False Distance Vector v5=1/7	Wormhole attack t1=1	CM_{51}=1 LCM_{51}=0
Spoofing v6=1/7	Spoofing t1=1	CM_{61}=1 LCM_{61}=0
Routing messages disclosure v7=1/7	Eavesdropping t1=1	CM_{71}=1/2 LCM_{71}=1/2

In above discussion, a new evaluation method is introduced for ad hoc routing protocol. Quantitative risk evaluation model could be used as a tool to conduct comparison between different routing protocols. It offers clear view on the strength of a secure system.

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 Conclusion

In this dissertation, we proposed MLASS, Multi-Level Adaptive Security System, which is capable of dealing with multilevel data and mobile ad hoc routing security and examines its feasibility for performance evaluation with single level security systems. In previous sections, we explained the structure of MLASS that deploys multi-level security technology, cryptography and steganography to provide adaptable and flexible security services for data and its distribution; then we constructed CB-MLDS, the secure content-based data processing subsystem that provides multilevel security services to the data being distributed; we also presented, verified and evaluated MOSAR, a mobile multilevel on-demand secure ad hoc routing protocol.

Through the simulations, we can conclude that MLASS shows the feasibility of integrating multilevel security into data security and routing security at the same time. CB-MLDS and MOSAR are computationally efficient and reasonably robust against security attacks. Though the potential of providing additional security through the use of multilevel routing is considered on a theoretical basis, the real performance evaluation of improvement in security can only be obtained using a real world network system with multilevel security in a controlled environment. This is beyond the scope of this study that is sharply focused on the development of a multilevel security system, and its performance evaluation in a simulated networking environment.

7.2 Future Work

In addition to the coverage in this dissertation on introducing the design of Multilevel Adaptive Security System, the experiments conducted on Content-Based Multilevel Data Security, and the simulations on Mobile Multilevel On-Demand Secure Ad Hoc Routing, the following issues should be further studied and implemented:

- Set up attack protocols for Performance Evaluation in CB-MLDSS subsystem, and collect breaking probabilities from real world for to establish the feedback database.
- The current implementation uses just three levels of trust for the nodes in an mobile ad hoc network: SECRET, CONFIDENTIAL and RESTRICTED. In the future, we would like to extend the system to support a finer granularity of trust levels. Also, the current implementation excludes the unknown nodes from participating in the routing process. We would like to explore a mechanism that allows the trust levels to be derived through certain trust relationships.
- Integrates the two subsystems, CB-MLDSS and MOSAR, and evaluate the overall performance for MLASS.

REFERENCES

[1] C. E. Perkings, *Ad Hoc Networking*. Upper Saddle River: Addison-Wesley, 2001.

[2] C. Siva Ram Murthy and B.S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*. Upper Saddle River: Prentice Hall, 2004.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," in *Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking*, 2002.

[4] K. Sanzgiri et al., "A secure routing protocol for ad hoc networks," in *Proceedings of the Tenth IEEE International Conference on Network Protocols*, 2002, pp. 78-87.

[5] Defense Information System Agency, Department of Defense, March 2003, http://www.disa.mil.

[6] S. Yi, P. Naldurg, and R. Kravets, "A security-aware routing protocol for wireless ad hoc networks," in *Proceedings of ACM MOBIHOC 2001*, October 2001, pp. 299-302.

[7] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Upper Saddle River: Prentice Hall, 1999.

[8] P. Wayner, *Disappearing Cryptography -- Information Hiding: Steganography & Watermarking*. San Francisco: Morgan Kaufmann Publishers, 2002.

[9] P. Papadimitratos and Z.J. Haas, "Secure routing for mobile ad hoc networks," in *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, January 2002.

[10] M. Brown et al., "PGP in constrained wireless devices," in *Proceedings of Ninth USENIX Security Symposium*, August 2000, pp. 247-261.

[11] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing in mobile wireless ad hoc networks," in *Proceedings of fourth IEEE Workshop on Mobile Computing Systems and Applications*, 2002, pp. 3-13.

[12] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proceedings of *ACM Workshop on Wireless Security*, 2002, pp. 1-10.

[13] P.Papadimitratos and Z.Haas, "Secure routing for mobile ad hoc networks," In Proceedings of *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, 2002.

[14] W.-P. Lu, "A model for multilevel security in computer networks," *IEEE Transactions On Software Engineering*, vol. 16, no. 6, June 1990.

[15] R. K. Thomas and R. S. Sandhu, "A trusted subject architecture for multilevel secure object-oriented databases," *Transactions On Knowledge And Data Engineering of IEEE*, vol.8, no.1, February 1996.

[16] R. Graubart, "The integrity-lock approach to secure database management," *IEEE Symposium on Security and Privacy*, 1984.

[17] B. Thuraisingham and W. Ford, "Security constraint processing in a multilevel secure distributed database management system," *Transactions On Knowledge And Data Engineering of IEEE*, 1995, pp. 274-293.

[18] R. A. Griffith and M. E. McGregor, "Designing and operating a multilevel security network using standard commercial products," May 2004, http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper037/sctycon2.pdf.

[19] V. Atluri et al., "Database security: status and prospects," in *Multilevel Secure Transaction Processing: Status and Prospects*, P. Samarati and R. Sandhu, Ed. Chapman & Hall, 1997.

[20] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications*, February 1999.

[21] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp.120-126, 1978.

[22] Opnet Technical Staff, *Manual of Opnet Modeler*, Opnet, 2004.

[23] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," in *Mobile Computing*, T. Imielinski and H. Korth, Ed. Kluwer Academic Publishers, 1996, pp. 153-181

[24] M. Sahinoglu, "Security meter: a practical decision-tree model to quantify risk," *IEEE Security & Privacy, Infrastructure Security*, vol. 3, no. 3, May/June 2005.