CRYPTO-AD-HOC NETWORK:
AN AD HOC NETWORK PROTOCOL EMBEDDED CRYPTOGRAPHY

By
KYUNGJOO SUH

A THESIS PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE

UNIVERSITY OF FLORIDA

2002
Copyright 2002

by

Kyungjoo Suh
ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my advisor, Dr. Abdelsalam (Sumi) Helal, for providing me the opportunity to work on this challenging topic and for offering continuous guidance, encouragement, and feedback during the course of this research. I would like to offer my appreciation to Dr. Dankel and Dr. Frank for agreeing to serve on my committee and for their careful review of this thesis. I also would like to thank Dr. Jinsung Kim and Dr. Myongsoo Park for their encouragement.

I would like to express sincere thanks to my fellow student Zhizhou Wang, Dr. Haejae Jung, and Diane for their support. I wish to thank David, Pushkar, Ameya, Madhav, Steve, and Edwin for their encouragement during this thesis work. I am grateful to thank Baldeep and Junhyo Bae for having discussion sections as a security research group. In addition, I thank Jinsuo and Choonhwa Lee, who helped me with computer problems.

I would like to offer my appreciation to my friend Hyunho Oh for his prayers and encouragement. I thank my friends Sunduk, Edna, Mary, Enid, Jungeun, Jione, Okehee, Meongchul Song and his wife, Reverend Son and Eunhee Goh, and Reverend Um for their support and for making my stay at the University of Florida a memorable one.

I would especially like to thank God for his guidance and love in my life. In addition, I would like to honor my father and my mother. I wish to offer my thanks to them and also my brother and sister for all their prayers, continual encouragement, emotional support, and endless love throughout my academic career.
# TABLE OF CONTENTS

ACKNOWLEDGMENTS ........................................................................................................ iii

LIST OF TABLES ................................................................................................................ vii

LIST OF FIGURES .............................................................................................................. viii

ABSTRACT ........................................................................................................................ ix

CHAPTERS

1. INTRODUCTION ......................................................................................................... 1
   1.1 Thesis Goal ........................................................................................................... 2
   1.2 Thesis Scope and Roadmap ................................................................................. 2
   1.3 Thesis Structure .................................................................................................. 3

2. ROUTING PROTOCOLS FOR AD HOC NETWORKS ............................................. 5
   2.1 Reactive versus Proactive Routing Protocols .................................................... 6
      2.1.1 Reactive Protocols .................................................................................... 6
      2.1.2 Proactive Protocols ............................................................................... 8
      2.1.3 Evaluation of Reactive versus Proactive Protocols ................................... 8
   2.2 The Hybrid Solution: the Zone Routing Protocol ............................................ 9
      2.2.1 Intrazone Routing versus Interzone Routing ............................................. 9
      2.2.2 Evaluation and Application of the Zone Routing Protocol ....................... 9

3. SECURITY MECHANISMS ...................................................................................... 11
   3.1 Vulnerabilities and Attacks in Ad hoc Networks .............................................. 12
      3.1.1 Passive versus Active Attacks .................................................................. 12
      3.1.2 Passive attacks ...................................................................................... 13
      3.1.2 Active attacks .................................................................................... 13
      3.1.2 External versus Internal Attacks ............................................................ 14
   3.2 Requirements for Secure Ad hoc Networks .................................................... 14
   3.3 Cryptographic Mechanisms ............................................................................. 15
      3.3.1 Public Key Authentication versus Secret Key Authentication ................. 16
         3.3.1.1 Public key authentication .......................................................... 16
         3.3.1.2 Secret key authentication ............................................................ 19
      3.3.2 Group Key Management ........................................................................ 22
      3.3.3 Secure Key Management ....................................................................... 22
3.3.4 Internet and Wireless Network Security Mechanisms ..................................... 23
  3.3.4.1 Internet Protocol Security (IP Security : IPSec) ....................................... 24
  3.3.4.2 Web security ............................................................................................. 26
  3.3.4.3 Security mechanism for mobile protocol.................................................. 27

4. EXISTING SOLUTIONS FOR SECURE AD HOC NETWORKS ...........................30

4.1 Existing Solutions ................................................................................................... 30
  4.1.1 Ad hoc Network Protocols from a Security Perspective ................................. 30
  4.1.2 Security Issues ............................................................................................... 31
    4.1.2.1 Confidentiality ...................................................................................... 34
    4.1.2.2 Integrity ............................................................................................... 35
    4.1.2.3 Authentication ..................................................................................... 36
    4.1.2.4 Trust relationship management and key management ............................. 37
    4.1.2.5 Availability .......................................................................................... 40

4.2 Limitations of Existing Solutions ........................................................................... 41
  4.2.1 Limitations of Existing Protocol from a Security Perspective ......................... 41
  4.2.2 Limitations of Existing Solutions for Security ................................................ 43
    4.2.2.1 Limitations of confidentiality techniques ............................................. 46
    4.2.2.2 Limitations of integrity assurance techniques ......................................... 46
    4.2.2.3 Limitations of authentication mechanisms ............................................ 47
    4.2.2.4 Limitations of key and trust relationship management mechanisms ...... 47
    4.2.2.5 Limitations of availability mechanisms ................................................ 48

5. PROPOSED APPROACH: THE CRYPTO-AD-HOC NETWORK ..........................50

5.1 Overview of the CRYPTO-AD-HOC Network ...................................................... 50
5.2 Importance of the CRYPTO-AD-HOC Network .................................................. 53
5.3 Design of the CRYPTO-AD-HOC Network .......................................................... 54
  5.3.1 Design Assumptions ....................................................................................... 54
  5.3.2 Overall Architecture and Components .......................................................... 55
  5.3.3 Authentication Mechanism .......................................................................... 57
  5.3.4 Key Management and Trust Relationship Management ................................ 58
    5.3.4.1 Key management .................................................................................. 58
    5.3.4.2 Trust relationship management ............................................................. 59
  5.3.5 Confidentiality Mechanism .......................................................................... 64
  5.3.6 Availability Mechanism ............................................................................... 64
    5.3.6.1 Intrusion detection mechanism ............................................................... 65
  5.3.7 Security Level ............................................................................................... 66
5.3.8 Routing ............................................................................................................. 67
  5.3.8.1 Routing discovery .................................................................................... 67
  5.3.8.2 Routing accumulation procedure ............................................................ 67
  5.3.8.3 Query control mechanisms and route maintenance ................................. 68
LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Lists of Existing Solutions in Terms of Security Service Criteria and above</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Viewpoints</td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>Lists of Limitations of Ad hoc Routing Protocols in Terms of Security</td>
<td>43</td>
</tr>
<tr>
<td>4.3</td>
<td>Lists of Limitations of Existing Solutions for Secure Ad hoc Networks</td>
<td>44</td>
</tr>
<tr>
<td>7.1</td>
<td>CRYPTO-AD-HOC Network Evaluations</td>
<td>71</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Zone Routing Protocol Architecture</td>
<td>10</td>
</tr>
<tr>
<td>3.1</td>
<td>The public key encryption from the viewpoint of confidentiality</td>
<td>17</td>
</tr>
<tr>
<td>3.2</td>
<td>Authentication via public key encryption</td>
<td>17</td>
</tr>
<tr>
<td>3.3</td>
<td>Digital signature as a manner of public key authentication</td>
<td>18</td>
</tr>
<tr>
<td>3.4</td>
<td>Secret key encryption from the viewpoint of confidentiality</td>
<td>19</td>
</tr>
<tr>
<td>3.5</td>
<td>Authentication via secret key encryption</td>
<td>21</td>
</tr>
<tr>
<td>3.6</td>
<td>Message digests as a manner of secret key authentication</td>
<td>21</td>
</tr>
<tr>
<td>4.1</td>
<td>Key management and trust management in each server and each node</td>
<td>39</td>
</tr>
<tr>
<td>5.1</td>
<td>Overview of the CRYPTO-AD-HOC network in terms of route discovery and security aspects</td>
<td>52</td>
</tr>
<tr>
<td>5.2</td>
<td>Overall picture of the CRYPTO-AD-HOC network</td>
<td>53</td>
</tr>
<tr>
<td>5.3</td>
<td>Overall architecture of the CRYPTO-AD-HOC network</td>
<td>56</td>
</tr>
<tr>
<td>5.4</td>
<td>Example of trust relationship among Certificate Authorities in a flexible bottom-up trust model</td>
<td>60</td>
</tr>
<tr>
<td>5.5</td>
<td>Example of certification links among Certificate Authorities and common nodes</td>
<td>61</td>
</tr>
<tr>
<td>5.6</td>
<td>Example of necessary certification from source to destination node regarding Certificate Authorities and common nodes</td>
<td>62</td>
</tr>
</tbody>
</table>
An ad hoc network is highly vulnerable to attacks from outside and inside. However, the current solutions do not meet the security requirements well in hostile environments. In this thesis, therefore, I attempt to find a better solution.

The security issue in an ad hoc network is an emerging area of research that is vital, but so far it has not been satisfactorily investigated. It is difficult to deal with security in ad hoc networks due to their characteristics: dynamic network topology, necessity of low-power consumption, and mobility. Research is being performed in several areas, and its scope falls into the area of secure routing and key management. Unfortunately, current research has problems caused from assumptions and other drawbacks. This thesis addresses these limitations and contributes improved concepts to current research, which I call the CRYPTO-AD-HOC network. Based on the spirit of cryptographic schemes and ad hoc networks, the CRYPTO-AD-HOC network uses extensive security and embedded security to aid the users of an ad hoc network.
The CRYPTO-AD-HOC network provides a number of security properties, such as confidentiality, authentication, integrity checking, availability, and nonrepudiation. The CRYPTO-AD-HOC is based on cryptography techniques. Between two broad categories, that is, secret key and public key algorithms, the CRYPTO-AD-HOC takes a public key infrastructure for a key management. The CRYPTO-AD-HOC network allows users to choose among multiple security levels, depending on several different types of security requirements. Two nodes, for example, require strong authentication, strong confidentiality, or no cryptographic protection. All these are related to key management and trust relation management using certification authorities in the CRYPTO-AD-HOC network. The CRYPTO-AD-HOC network is deployed using a flexible bottom-up trust model; it allows distributed trust management. In this scheme, autonomous certification authorities have peer-to-peer certification that provides flexibility so that no single compromised node can cause the entire network to be reconfigured.

To conclude, the CRYPTO-AD-HOC network provides a secure network to users employing a cryptographic mechanism, that is, public key infrastructure and a flexible bottom-up trust relationship management with which we can handle the malicious intention by isolating a no longer trusted node. Finally, the CRYPTO-AD-HOC network not only gives the security benefit to users who employ the ad hoc networks with low cost and low computation and network overhead, but also solves some restrictions and drawbacks of previous research.
CHAPTER 1
INTRODUCTION

An ad hoc network is an infrastructureless network in which each node acts as a host and router. Each node is responsible for forwarding packets to other nodes. The existing ad hoc networks do not properly work with respect to security and are highly vulnerable to attacks and threats in a hostile environment. It is difficult to merely apply a traditional network security solution to ad hoc networks because of their special properties, such as low bandwidth, limited battery life, transmission range, dynamic topology, mobile nodes, and decentralized administration. Mainly, the difficulties of dealing with security issues in an ad hoc network come from the key management and trust relationship management. These characteristics place a new demand on secure ad hoc networks [1].

Among existing ad hoc networks, the Zone Routing Protocol (ZRP) has proactive and reactive elements. In the Zone Routing Protocol, zones are introduced into the network. The Zone Routing Protocol consists of the Intrazone Routing Protocol (IARP) and the Interzone Routing Protocol (IERP). The Zone Routing Protocol is a solution that can restrict failures to smaller areas in a network. In terms of security, the zone routing information can be hidden to the outsider except the situation in which communication is done through the Interzone Routing Protocol.

This thesis presents a new solution for a secure ad hoc network, namely, the CRYPTO-AD-HOC network, which addresses the secure routing and cryptography. The CRYPTO-AD-HOC network offers immense security features to the ad hoc network user
without impairing the fast decision-making and low cost. The most valuable asset of this solution is presenting more secure features, thus aiding users to the generation of reliable links and trustworthy communication.

1.1 Thesis Goal

The goal of this thesis is to suggest a highly efficient security solution for an ad hoc network, namely, the CRYPTO-AD-HOC network, by establishing secure routing and cryptography. The CTYPTO-AD-HOC network focuses on presenting an improved and secure way of an ad hoc network against attacks in a highly vulnerable environment.

The secondary objective of this thesis is to provide a low-cost way to make fast decisions regarding security aspects in the reconfigurable wireless networks environment. This objective makes nodes join and leave the network frequently without disruption of other nodes’ communication. Therefore, the CRYPTO-AD-HOC network provides security benefits when deployed in certain circumstances in which fast decision-making and secure communication are required. These circumstances include tactical operations, national security, and law enforcement.

1.2 Thesis Scope and Roadmap

In this thesis, I rely on the following assumptions. First, developing some part of a secure routing protocol applied to any other Mobile Ad hoc Networks (MANET) solutions is impossible because it can cause unpredictable vulnerabilities by not designing security mechanisms with the basic routing protocol. Second, I restrict my research to Internet Protocol-based (IP-based) networks for secure routing. Third, I deploy a cryptographic mechanism, that is, key management and trust relationship management, and take an application-dependent approach. Fourth, among ad hoc
networks intended to be deployable anywhere without any existing infrastructure, I focus on a reconfigurable wireless network. A reconfigurable wireless network is different from other ad hoc networks by rapidly changing network topologies, which are influenced by network size, and node mobility.

In this thesis, I build my solution based on the hybrid ad hoc network solution. The reason I choose the hybrid solution is that table-driven protocols, that is, proactive protocols, are not appropriate; the constant and heavy routing information exchange causes overhead. On the other hand, in an on-demand routing protocol, sometimes called a reactive protocol, route information may not be available at the time of a route request. This non-availability of route information causes a significant delay or excessive control traffic. For providing confidentiality, authentication, and integrity checking, I deploy a public key infrastructure, which demands a trust relationship management. The trust relationship management is a crucial part for secure communication.

1.3 Thesis Structure

Current ad hoc networks are introduced in Chapter 2. I focus on classifying an ad hoc network in terms of reactive versus proactive routing protocols rather than introducing various protocols. To create a route on demand, but at a low search cost, causes the needs of the hybrid solution, namely, the Zone Routing Protocol.

Chapter 3 explains mobile security issues: the goal of security service and security issues introduced by mobility. In addition, I define vulnerabilities, attacks, and threats in ad hoc networks and indicate requirements for a secure ad hoc network. At the end of this chapter, I explain cryptographic techniques and security mechanisms in use, and I illustrate the security issue for a mobile protocol.
Chapter 4 illustrates some of the current suggested solutions for a secure ad hoc network and their assumptions. I evaluate current solutions and indicate the problems of current solutions, which introduce the necessity for the CRYPTO-AD-HOC network.

In Chapter 5, I introduce the CRYPTO-AD-HOC network as a novel and improved solution. In this chapter, I discuss the importance, the protocol design, the implementation details, and simulation details of the CRYPTO-AD-HOC network.

Finally, I draw conclusions, addressing some issues that are not in the current scope of the CRYPTO-AD-HOC network, and I provide a brief description of future research.
CHAPTER 2
ROUTING PROTOCOLS FOR AD HOC NETWORKS

The ad hoc network, called ubiquitous computing, forms a temporary infrastructureless network so mobile computer users with wireless communication devices can possibly set up a short-lived network just for communication. Therefore, no centralized administration exists. In addition, limited transmission range causes multihop routing in which a mobile node acts as a router and a host. Ad hoc networks include the following characteristics: dynamic topology, limited CPU capacity, limited battery power and bandwidth, and unidirectional links because of different transmission ranges for different mobile nodes. The requirements and challenges of ad hoc routing are as follows: distributed operation, supply for loop freedom, avoiding waste of bandwidth or CPU power consumption, security, Quality of Service (QoS) support, and stability of routes [1].

Among ad hoc networks, a Reconfigurable Wireless Network (RWN) is an ad hoc network characterized by rapidly changing the node constellation and a highly mobile network without relying on a pre-existing fixed network infrastructure. The mobile platforms on which the network nodes reside are cars, planes, ships, and tanks. In the Reconfigurable Wireless Network environment, nodes show freely migrating behavior within some areas, and they dynamically create links with others. Communication between nodes is restricted only by connectivity limitations and subject to security
provisions. A time-varying network topology results from different node mobility patterns that vary with time and position.

A Reconfigurable Wireless Network is a peer-to-peer network that allows direct communication between two nodes. However, multihop routing is used if no direct link between the source and the destination nodes is available. To increase reliability of the network and to adjust to a frequently changing network, the following characteristics are required: robust routing, mobility management, and adaptive algorithm.

2.1 Reactive versus Proactive Routing Protocols

Routing protocols for ad hoc networks are classified as either proactive or reactive. The remaining parts are shown in detail in the next section.

2.1.1 Reactive Protocols

Reactive protocols, called source-initiated routing protocols, are on-demand routing, which means the route to a specific destination is computed only when needed. Reactive protocols invoke routes only when desired on demand by the source node [2]. Examples include Ad hoc On-demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), and Temporally-Ordered Routing Algorithm (TORA).

The Ad hoc On-demand Distance Vector Routing is a reactive protocol. When a route is necessary, the Ad hoc On-demand Distance Vector Routing requests a route. Furthermore, in the Ad hoc On-demand Distance Vector Routing, nodes are not required to maintain routes to destinations that are not communicating. The Ad hoc On-demand Distance Vector Routing is an example of a distance vector routing protocol. The Ad hoc On-demand Distance Vector Routing uses sequence numbers to indicate the freshness of a route and to avoid routing loops. The features of the Ad hoc On-demand Distance
Vector Routing protocol are as follows: When a node needs to find a route to another node, it broadcasts a Route Request (RREQ) message to all its neighbors. The Route Request message is flooded through the network until it finds the destination or a node that has a fresh route to the destination. At this time, the Route Request message creates temporary route table entries for the reverse route. If the Route Request message finds a destination or a route, a Route Reply (RREP) message unicasts back to the source through the temporary path that is the reverse of the Route Request message. At this point, the Route Reply creates routing table entries for the destination that will expire after a certain amount of time.

The Dynamic Source Routing is also a reactive routing protocol. The fact that the Dynamic Source Routing is a source routing makes the headers of the data packets carry the addresses of the nodes through which the packet passes. Therefore, the source has to recognize the complete hop sequence to the destination. In contrast to forward data packets, intermediate nodes have to track only of their immediate neighbors. The protocol works as follows: When a route is necessary, the Dynamic Source Routing floods the Route Request packet. The packet is propagated over the network until it discovers the destination or a node with a route to the destination. In the Dynamic Source Routing, each node has its own route cache to store its known route. Therefore, when a node receives a Route Request packet, it searches its route cache to find a route to the destination. The Route Request packet and Route Reply packet have the hop sequence to go to the destination. If a route exists, a Route Reply packet with the proper hop sequence to the destination is unicast back to the source node. If there is no route to the
destination, a node forwards the Route Request packet after first having added its address to the hop sequence.

2.1.2 Proactive Protocols

Proactive protocols, called table-driven routing protocols, attempt to maintain a consistent view of the network, maintain up-to-date routing information whenever there is a topology change, and continuously evaluate the routes within the network [2]. Some examples include Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), and Open Shortest Path First (OSPF).

The Destination Sequenced Distance Vector is a proactive protocol so that routing updates are broadcast periodically to keep the routing table updated. In addition, the Destination Sequenced Distance Vector is a hop-by-hop distance vector routing protocol so that each node maintains a routing table that contains the next hop to the destination and the number of hops. The Destination Sequenced Distance Vector uses sequence numbers to indicate how much route is fresh so that this network has loop freedom. The route that has a higher sequence number is more favorable. If the sequence number is equal, the route that has the lower hop count is preferred.

2.1.3 Evaluation of Reactive versus Proactive Protocols

The reactive protocols outperform the proactive protocols in terms of throughput and delay. The reactive algorithm is suitable for the environment with limited bandwidth capacity because the proactive algorithm depletes many resources to update paths.

Even though the reactive operation is more desirable in ad hoc networks, the reactive approach has drawbacks in real-time environment: long delay when requested and immense control traffic in the reactive global search procedure [3].
Proactive schemes cause a tremendous waste of network capacity in the Reconfigurable Wireless Network environment. In the Reconfigurable Wireless Network, the topology change is more frequent, thus a proactive scheme uselessly consumes network capacity to keep the routing information that was never used.

### 2.2 The Hybrid Solution: the Zone Routing Protocol

The solution is creating the route on demand, that is, reactive, but at a low search cost. This way guarantees no waste of network capacity. Therefore, we need the introduction of a hybrid solution, namely, the Zone Routing Protocol by Hass [4].

#### 2.2.1 Intrazone Routing versus Interzone Routing

In the Zone Routing Protocol, the zone means node connectivity (hops) and does not mean physical distance. The Zone Routing Protocol consists of two routing protocols, namely, the Intrazone Routing Protocol and the Interzone Routing Protocol. The Intrazone Routing Protocol used within each zone is a proactive protocol. The Interzone Routing Protocol is used between zones to find routes, and it is a reactive protocol.

The architecture of the Zone Routing Protocol is shown in Figure 2.1. In this Figure, the Neighbor Discovery Protocol (NDP) informs the Intrazone Routing Protocol when a link to a neighbor is established.

#### 2.2.2 Evaluation and Application of the Zone Routing Protocol

The Zone Routing Protocol limits the search cost by limiting the scope of the proactive procedure to its own neighborhood. If frequent route requests exist, large routing zones cause more proactive procedures and produce low overhead. The Zone Routing Protocol shows minimum delay in larger routing zones. On the other hand, in the Zone Routing Protocol, changes in the network topology have only a local effect.
Figure 2.1: Zone Routing Protocol Architecture\textsuperscript{1}

\textsuperscript{1} Source: [4]
CHAPTER 3
SECURITY MECHANISMS

Computer network and information security has three aspects: security attacks, security goals, and security mechanisms. The objective of the security service is to achieve confidentiality, authentication, integrity, nonrepudiation, access control, and availability [5].

1. Confidentiality: Only authorized parties can access and disclose transmitted information or the information in a computer.

2. Authentication: The origin of a message should be correctly identified.

3. Integrity: Only authorized parties can modify, delay, or replay transmitted information or the information in a computer.

4. Nonrepudiation: Neither the sender nor the receiver of a message can deny the transmission.

5. Access Control: The access to resources of information may be controlled by or for the target system.

6. Availability: When needed, the assets of a computer system are available to authorized parties.

In a wireless environment, the threats to confidentiality, integrity, and nonrepudiation are greatly increased. Furthermore, being near a target increases the risk of eavesdropping and transmitting. The hardware limitations, such as limited battery power and low network bandwidth, make the situation worse by causing denial of service, for example, resource exhaustion or depletion. Achieving security goals was threatened by vulnerabilities, threats, and attacks in ad-hoc networks. These are the topics of discussion in the next section.
3.1 Vulnerabilities and Attacks in Ad hoc Networks

In ad hoc networks, the severe vulnerabilities come from the poor physical security of the mobile nodes, for example, theft of nodes, which can be compromised or tampered. Furthermore, due to limited battery power, a mobile node is limited by the computational power, which means if a security mechanism causes much computation, we cannot use it.

The flow of information from a source to a destination could be attacked. The following categories point out the generic types of attack behaviors and the security targets from an angle by looking at the transmitted information [6].

1. Interception: The target of interception is confidentiality, that is, an unauthorized party gains access to information.

2. Fabrication: Authenticity can be harmed by fabrication thereby an unauthorized party inserts counterfeit information into the system.

3. Modification: The information integrity can be in danger by modification. An unauthorized party accesses, as well as tampers with, an asset. The result is an unauthorized effect and the altered, delayed, or reordered message.

4. Interruption: The information is unavailable, unusable, or destroyed by interruption.

These attacks are categorized in terms of passive attacks and active attacks with respect to attack characteristics. Moreover, by viewing who is an attacker, we can distinguish external attacks from internal attacks.

3.1.1 Passive versus Active Attacks

The nature of passive attacks is eavesdropping on transmission of information or the monitoring of transmission. The active attacks have the characteristics of modification of information or the creation of a false data stream [7-9].
3.1.1.1 Passive attacks

The passive attacks break confidentiality by interception. They are divided into two categories: release of message contents and traffic analysis. In handling these attacks, we usually focus on prevention because it is difficult to detect these kinds of attacks. In ad hoc networks, even though the passive attacker does not disrupt the operation, it attempts to discover valuable information, which includes disclosing routing data, that is, location of nodes and network topology. The following categories show passive attacks.

1. The release or disclosure of message contents: An adversary can gather the contents of the message.
2. The traffic analysis: An adversary is able to guess the nature of communication. Even though the adversary does not know the exact information, he can obtain the frequency and length of messages. As a result, he can determine the location and identity of the hosts.
3. Location disclosure: An attacker knows about location of nodes and network topology from obtaining routing information in the ad hoc network.

3.1.1.2 Active attacks

The active attacks include fabrication, modification, and interruption by causing harm on authenticity, integrity, and availability. The security goal against active attacks rests on detecting them and recovering them from any delay or disruption. Especially in the ad hoc network environment, the following active attacks cause problems.

1. Denial of Service: An intruder tries to prevent or inhibit the normal use or management of communication facilities, especially routing in ad hoc networks. This attack involves degrading network performance by overloading the network with messages or disruption of the network. This attack disables the security service by directing all messages to detection mechanisms. In an ad hoc network, this attack includes the exhaustion of chosen nodes. It is difficult to prevent this attack.
2. Routing table overflow: An adversary attempts to create routes to nonexistent nodes so that new routes cannot be created or unnecessary routes overwhelm the protocol. A proactive routing protocol is more
vulnerable to routing table overflow than a reactive protocol because a proactive protocol gathers routing information periodically.

3. Modification of location information: Not only is the integrity of a transmitted message crucial but also the integrity of routing information is crucial to correctly maintain the routing in an ad hoc network.

4. Replay: This attack takes place when the attacker captures a data entity and then retransmits to produce an unauthorized effect.

5. Masquerade (Impersonation): An intruder pretends to be a different entity. This attack therefore usually happens with other active attacks, for example, modification and replay.

6. Black hole: In the protocol that uses the shortest path algorithm to find the proper routing, a malicious node pretends to have the shortest path to a destination node to which it attempts to intercept. Once the attacker intercepts between communications, he deletes the packets. As a result, Denial of Service or other active attacks can be created.

3.1.2 External versus Internal Attacks

Intruders or attackers from the outside cause external attacks. External attacks cause network congestion, routing loops, or sending wrong routing information. Internal attacks are more complicated than external attacks because usually internal malicious nodes already have permission from a security mechanism. Therefore, it is difficult to find out what is wrong. In the context of providing a secure private network, we cannot ignore this kind of attack from an insider.

3.2 Requirements for Secure Ad hoc Networks

With respect to security, secure ad hoc routing has to satisfy several requirements, such as isolation, self-stabilization, Byzantine robustness, certain discovery, location privacy, and lightweight computation [9-12]. The following list details the definition of requirements:
1. **Isolation**: A routing protocol must have the ability to detect malicious nodes and isolate them from routing. These abilities result in making the protocol immune to misbehaving nodes.

2. **Self-stabilization**: This ability is the property with which a routing protocol automatically recovers from problems within a finite time. Because of this property, we also detect the attacker easily if he attempts to cause damage continuously.

3. **Byzantine robustness**: Even though there is an attack and some of the nodes involved in routing are disrupting its functions, a routing protocol can work correctly.

4. **Location privacy**: The protocol has to protect location information of nodes in a network.

5. **Lightweight computation**: To protect against Denial of Service attacks, low computation is required. This property is essential to low power consumption in ad hoc networks in which mobile nodes are often laptops and Personal Data Appliances/Assistants (PDAs).

### 3.3 Cryptographic Mechanisms

Cryptographic mechanisms include algorithms and keys. Cryptographic algorithms consist of secret key algorithms and public key algorithms. In secret key algorithms, also called symmetric algorithms, the same secret key is used by the sender and the receiver. Public key algorithms, called asymmetric algorithms, use a related key pair, namely, a secret key and a public key. The sender uses one from a key pair of a secret key and a public key, and the receiver uses another from the key pair. In public key algorithms, only a specific person (a sender or a receiver) knows a private key. On the other hand, persons in the networks may know more than one person’s public key. The key management (secure key distribution) is an important issue in a cryptographic system [5-13].

Usually secret key algorithms are faster than public key algorithms. On the other hand, public key algorithms are easier to distribute than secret key algorithms. Based on
these characteristics, secret key algorithms are used as a solution for handling the actual data, and public key algorithms are used for distributing keys.

### 3.3.1 Public Key Authentication versus Secret Key Authentication

Authentication is a necessary characteristic for security management in an ad hoc network because authentication is the process of proving identity as a member. Public key algorithms or secret key algorithms can accomplish this authentication.

#### 3.3.1.1 Public key authentication

Public key authentication can be classified into two categories. The first category is authentication via public key encryption. The second category is digital signatures.

In a public key cryptography scheme, each person has two mathematically related keys: a private key and a public key. In this mechanism, only the receiver knows the value of his private key, and the public key is known to as many persons as possible.

From the viewpoint of confidentiality, in the public key encryption, the sender transmits confidential messages to the receiver by encrypting them using the receiver’s public key ($Pr$: where $P$ represents the public key, $r$ represents the receiver). The receiver decrypts the messages using his secret key ($Sr$: where $S$ represents the secret key, $r$ represents the receiver). Through encryption algorithms, the sender can prevent all others except the receiver from reading the sender’s data, which means that the sender and the receiver achieve confidentiality. As a result, only the receiver is the person who possesses the corresponding private key and decrypts the message. On the other hand, anyone who possesses the receiver’s public key can send the receiver a confidential message. The public key encryption is shown in Figure 3.1.
Figure 3.1: The public key encryption from the viewpoint of confidentiality

Sender transmits message by encrypting using the public key of the receiver, that is, Cipher text = E \{Pr, Plaintext\}

Receiver decrypts message by using Sr: secret key of the receiver, that is, Plaintext = D \{Sr, Cipher text\}

Figure 3.2: Authentication via public key encryption

Receiver requests the encryption of random number \(r_1\)

Sender transmits random number \(r_1\) by encrypting using the secret key of the sender, that is, Cipher text = E \{Ss, \(r_1\)\}

Receiver decrypts by using Ps: Public key of the sender and verifies random number \(r_1\), that is, \(r_1 = D \{Ps, Cipher text\}\)

Figure 3.2 illustrates authentication by public key encryption. From the viewpoint of authentication, the receiver verifies a random number \(r_1\) by using the public key of the sender. In this way, only the sender can generate authentication that verifies him as the sender because only the sender has access to the corresponding private key (secret key).
The second category of public key authentication is digital signatures. Digital signatures mean the resulting cipher text that comes from signing a message, which involves performing public key transformations on a plaintext message with a private key. In other words, the sender verifies himself to the receiver by performing a public key transformation on some plaintext message using his private key, and sends the result, that is, authenticated cipher text, to the receiver. The receiver verifies the message by performing an associated public key transformation on the received cipher text using the sender’s public key. Before this point, it is important to securely get the public key and that is the issue of key management. If this transformation produces the expected result, then the receiver knows that the sender is correct, and this system verifies the sender to the receiver. Figure 3.3 shows the digital signature scheme.

**Figure 3.3: Digital signature as a manner of public key authentication**

Sender requests the encryption of Plaintext

Sender sends message by encrypting using the secret key of the sender, that is, Cipher text = \( E_{Ss} \text{ Plaintext} \)

Therefore, the sender provides authentication

Receiver decrypts by using \( Ps: \text{Public key of the sender} \) and verifies the message, that is, Plaintext = \( D_{Ps} \text{ Cipher text} \)
3.3.1.2 Secret key authentication

The secret key authentication can be classified into two categories. One category is authentication via secret key encryption, and the other category consists of message digests. In the secret key cryptography, it is assumed that both the sender and receiver share the secret key and that they must agree on a specific secret key encryption algorithm to use.

From the point of view of confidentiality, in secret key encryption the sender transmits confidential messages to the receiver by encrypting them using the key shared by both the sender and the receiver. \((K_{sr}:\) where \(K\) represents the shared key by the sender and receiver, \(s\) represents the sender, \(r\) represents the receiver). Only the other person, who is the receiver, can decrypt the messages using the same key, that is, their shared key \((K_{sr})\). In this scheme, there is no reason to keep the algorithm secret. Therefore it is more important to manage the key securely. Figure 3.4 shows secret key encryption.

\[
\text{Sender transmits message by encrypting using the key that is shared by both the sender and receiver, that is, Cipher text} = E\left(K_{sr}, \text{Plaintext}\right)
\]

\[
\text{Receiver decrypts message by using } K_{sr}: \text{shared key, that is, Plaintext} = D\left(K_{sr}, \text{Cipher text}\right)
\]

Figure 3.4: Secret key encryption from the viewpoint of confidentiality
When you want to see the secret key encryption from the point of view of authentication, the receiver verifies a random number $r_1$ by using the shared key. In contrast, public key encryption uses the public key of the sender. Using this method, only the sender can generate authentication that verifies him as the sender. The reason is that only the sender and receiver have access to the corresponding shared key. On the other hand, in public key authentication, the sender has access to the private key (secret key). In secret key authentication, it is necessary to have mutual authentication because the sender and receiver share the key. Figure 3.5 illustrates authentication via secret key encryption. In this diagram, the solid arrows ( ) show the authentication process from the sender to the receiver using the random number $r_1$, and the dotted arrows ( ) show the opposite process using $r_2$.

The second category of secret key authentication consists of the message digests. The message digests mean the smaller fixed part of the data that are unique and computed arbitrarily from the message. The assumption of the message digest is that both the sender and receiver share a single secret key, and they have to agree on a specific message digest algorithm. In this mechanism, the sender verifies himself to the receiver by asking to compute the message digest of a proper value using the shared secret key. Then the receiver verifies the message digest. If the message digest, which is computed by receiver using the sender’s timestamp, is equal to the message digest that came from the sender, then the receiver verifies the sender. This process authenticates the sender to the receiver. Mutual authentication is necessary. The one-way process of message digest is shown in Figure 3.6.
1) Receiver requests the encryption of random number $r_1$

2) Sender transmits $r_1$ by encrypting using the shared key, that is, Cipher text 
$$= E\{K_{sr}, r_1\}$$
Therefore, the sender provides authentication to the receiver.

3) In addition, the sender requests the encryption of random number $r_2$

6) The receiver sends $r_2$ by encrypting using the shared key, that is, $E\{K_{sr}, r_2\}$
So, the receiver provides authentication to the sender.

4) Receiver step 1: decrypts by using $K_{sr}$ and verifies, that is, $r_1 = D\{K_{sr}, Cipher \text{ text}\}$ - equation 1

5) step 2: If the result of equation 1 is equal, encrypts $r_2$ using $K_{sr}$

Figure 3.5: Authentication via secret key encryption

1) The sender transmits his timestamp and the message digest computed with shared key and timestamp, that is, sender's timestamp and $MD\{K_{sr} - s + timestamp\}$
Therefore, the sender provides authentication

2) Also, the sender requests the receiver to verify message digest

3) Verifies message digest, that is, compute the receiver's own $MD\{K_{sr} - r + sender's \text{ timestamp}\}$ and compare with received $MD\{K_{sr} - s + timestamp\}$
if equal, the sender is verified

where, $K_{sr-r}$: shared secret key of the receiver $K_{sr-s}$: shared secret key of the sender

Figure 3.6: Message digests as a manner of secret key authentication
3.3.2 Group Key Management

The Group Key Management Protocol concentrates on establishing and managing a common key among all group members. A group key is used for encryption and group authentication, but it is not sufficient for individual authentication. The group controller has responsibility for managing the group keys. For group key distribution, three approaches exist. In centralized approaches, only one group controller exists. In distributed subgroup approaches, the management of the group is distributed among subgroup managers. In distributed approaches, the members themselves distribute keys so that no explicit group controller exists [14].

3.3.3 Secure Key Management

When keys are distributed to entire networks, it is important to manage the key appropriately. Only appropriate persons have to know or share the keys to manage the key securely. In public key cryptography, the two parties obtain each other’s public key through certification. On the other hand, in secret key cryptography, only two parties can share their secret keys.

Even though it is easier to securely manage keys in public key cryptography than in secret key cryptography, distributing public keys securely is an important issue. The reason to distribute keys securely is that someone can pretend to be a communicating party, intercept the message, and, at the end, substitute their public keys. Therefore, it is necessary to authenticate the public key itself or authenticate the message that contains the public key.

A Certificate Authority is the trusted third party who digitally signs someone’s (X’s) public key ($P_x$) in the form of a public key certificate, that is, authenticated cipher text $= E\{Sca, P_x\}$ where $Sca$ means *Secret key of Certificate Authority* and $P_x$ means
someone’s (X’s) public key. In addition, the assumption is that everybody knows \( Pca \) (public key of Certificate Authority). Therefore, one can verify someone else using \( Pca \) and get someone else’s (X’s) public key (\( Px \)). Moreover, this system authenticates a Certificate Authority to others.

The Public Key Infrastructure (PKI) has the following goal: secure, convenient, and efficient discovery of public keys. Various types of the Public Key Infrastructure are proposed: using a single Certificate Authority, an oligarchy of Certificate Authorities, configured Certificate Authorities and delegated Certificate Authorities, a top-down trust model, an up-cross-down trust model, and a flexible bottom-up trust model. For scalability, Certificate Authorities usually have a hierarchy. Therefore, a user might have a copy of its public key to traverse the layer of a hierarchy.

The X.509 is one of the standards for the Public Key Infrastructure. The X.509 defines a framework for authentication services by the X.500 directory. Each certificate contains the public key of a user and is signed with the private key of a Certificate Authority. The X.509 certificate format is important because it is used in various web security mechanisms, such as Secure Multipurpose Internet Mail Extension, Internet Protocol Security, Secure Socket Layer/Transport Layer Security, and Secure Electronic Transaction [11].

3.3.4 Internet and Wireless Network Security Mechanisms

For Internet communication, application-specific security mechanisms, such as Secure Sockets Layer for Web access, Kerberos for client/server, and Pretty Good Privacy for electronic mail, have been developed in an application area for Internet communication. On the other hand, an IP-level security mechanism is implemented in the Internet Protocol Security.
3.3.4.1 Internet Protocol Security (IP Security: IPSec)

The Internet Protocol Security (IP Security: IPSec) is an IP-level security mechanism and has the following functions: authentication, confidentiality, and key management. Authentication enables an identified source in the packet header to transmit a packet. Confidentiality means communicating nodes can encrypt messages to prevent eavesdropping. Key management assures that keys are exchanged in a secure manner. The IPSec enables a system to choose required security protocols, select the algorithms, and use cryptographic keys [6, 13].

The IPSec provides security services, such as access control, connectionless integrity, data origin authentication, rejection of replayed packets, and confidentiality, through the following two protocols: the Authentication Header (AH) and the Encapsulating Security Payload (ESP). The Security Association (SA) is a one-way relationship between a sender and a receiver. In addition, security association is uniquely identified by destination address in the header of any IP packet, such as the Internet Protocol Version 4 (IP version 4: Ipv4) datagram or the Internet Protocol Version 6 (IP version 6: IPv6) packet. Therefore, the security association is a critical concept for authentication and confidentiality. The IPv6 is different from the IPv4. The IPv6 becomes more prevalent and the next generation of the Internet Protocol because it provides functional enhancements to accommodate the higher speeds and the mix of data streams, including graphic and video. The size of the addresses to specify a source or destination makes a big difference: 128 bits in the IPv6 versus 32 bits in the IPv4.

The Authentication Header is an authentication protocol designated by the header. The two parties must share a secret key because authentication is based on the use of a Message Authentication Code (MAC). Therefore, the Authentication Header provides
integrity, authentication, filtering traffic, and prevention of the address spoofing attacks and replay attack. The Encapsulating Security Payload is a combined encryption and authentication protocol, where authentication is optional and designated by the format of the packet. Therefore, it provides confidentiality, and it optionally provides authentication.

In the IPSec, the key management is performed manually or automatically. The Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley) is the default automated key management protocol for the IPSec. The Internet Security Association and Key Management Protocol (ISAKMP) consists of a set of message types that support the use of key exchange algorithms. By defining procedures and packet formats, the ISAKMP establishes, negotiates, modifies, and deletes security associations. During the process of establishing a security association, the ISAKMP defines a payload whose formats provide a consistent framework independent of the specific key exchange protocol and encryption/authentication mechanism. The Oakley is the key exchange algorithm that retains the advantages of the Diffie-Hellman algorithm and counters its weaknesses. The Oakley algorithm employs cookies to thwart clogging attacks. It also employs a one-time, unique message number, called nonce, in each message to thwart replay attacks. In clogging attacks, an attacker forges the source address of a legitimate user and sends a public Diffie Hellman key to the victim. The victim attempts to compute the secret key so that it is clogged with useless work. However, the ISAKMP/Oakley is useful only where a pre-existing security relationship exists by manual configuration or by using a certificate authority.
3.3.4.2 Web security

The Web faces a variety of security threats, for example, modification of user data, eavesdropping on the network, flooding machine with bogus threats, and impersonation of legitimate users. The various solutions provide security services, however, they differ in terms of their scope of applicability and their relative location within the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack: network level, transport level, and application level [5, 6, 10, 11].

Using the IPSec at the IP layer is a network level solution and has advantages: The IPSec has a filtering capability so that only selected traffic cause overhead for processing. In addition, the IPSec provides a general purpose approach and it is transparent to users.

Another approach is using the Secure Sockets Layer (SSL) and the Transport Layer Security (TLS). This approach is implemented above TCP layer. Using the SSL or the TLS is therefore a transport level solution and general purpose approach. The SSL or the TLS can be implemented as part of the underlying protocol suite or embedded in a specific package, such as Netscape and Microsoft Explorer browsers.

Application-specific security services, such as Secure Electronic Transaction (SET), Kerberos, Secure/Multi-Purpose Internet Mail Extension (Secure MIME: S/MIME), and Pretty Good Privacy (PGP), are embedded within the particular application. This approach has an advantage in that the security service can be tailored to the specific needs.

Electronic mail is the network-based application and has grown dramatically. The PGP is originally designed for electronic mail, and it is also used for file storage applications. The PGP provides confidentiality and authentication by encrypting and
signing messages using the Rivest-Shamir-Adelman (RSA) and the International Data Encryption Algorithm (IDEA), which is a symmetric key cipher. A keyring is a list of the public keys of all those with whom the user corresponds, and a keyring is signed by the user’s own private key. The PGP users maintain a keyring and exchange keyrings with each other. When a key is added to another person’s keyring, a key is assigned a degree-of-trust attribute, such as completely trusted, marginally trusted, untrusted, and unknown. The limitation of the PGP comes from the fact that a user’s keyring can contain false public keys. For example, B is supposed to trust A, but B is fooled by an A’s impersonator, that is, C. C (an impersonator of A) can forge A’s signature and send messages to B. In this case, B accepts the message from C as coming from A, and C can read any encrypted message from B to A. A serious flaw is that everyone who relied on B to obtain A’s key is also fooled.

3.3.4.3 Security mechanism for mobile protocol

The Wireless Personal Area Network (WPAN) covers a short range within a 10-meter radius. Bluetooth supports security service in the Wireless Personal Area Network and provides point-to-point and point-to-multipoint communication. Bluetooth networks are categorized into piconet, scatternet, and multipoint. Bluetooth security aspects are as follows: 128-bit public/private key authentication, streaming cipher up to 64-bit, and four basic keys, that is, 48-bit fixed public address unique to a device, 128-bit random number per transaction, 128-bit secret key for authentication, and variable length bits secret key from 8 to 128 bits for encryption.

The Wireless Local Area Network (WLAN) is a wireless version of the Local Area Network (LAN) covering a limited area such as within a building or a group of buildings, and provides access to the LAN within 100-meter radius. The 802.11 is the
Institute of Electrical and Electronics Engineers (IEEE) standard for the wireless LAN. The 802.11b is proposed for a faster data rate and a more robust communication. The Wired Equivalent Privacy (WEP) is a link layer security protocol built into the IEEE 802.11b standards. The WEP relies on a secret key that is shared between a mobile station and an access point. The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified. The WEP uses the RC4 encryption algorithm, which is a variable key-size stream cipher with byte-oriented operations designed by Rivest and based on the use of a random permutation. Security for 802.11 networks consists of three components: the authentication mechanism or framework, the authentication algorithm, and data frame encryption. The 802.1x is an IEEE standard that provides an authentication framework for 802-based LANs. The 802.1x takes advantage of Extensible Authentication Protocol (EAP). The EAP messages are encapsulated in 802.1x messages and called the EAPOL, that is, EAP over LAN. 802.x authentication consists of three components: The supplicant (client software), the authenticator (access point), and the authentication server (a Remote Authentication Dial-in User Service server). The 802.1x leaves key distribution or management unspecified. The 802.x has the potential to simplify security management for large wireless deployments. In addition, the IEEE 802.1x is an important feature of Microsoft Corporation’s new Windows XP OS, and it provides a network login capability between PCs.

The Wireless Wide Area Network (WWAN) covers an area within 10-kilometer radius. The Wireless Application Protocol (WAP) is an application framework and network protocol for wireless devices. The Wireless Transport Layer Security (WTLS) is
used in the Wireless Wide Area Network environment, and it is based on Transport Layer Security, that is, the Secure Socket Layer. The WTLS is optimized for use over narrow-band communication channels. The main purpose of the WTLS is to establish symmetric keys and encrypt data [11-13].
CHAPTER 4
EXISTING SOLUTIONS FOR SECURE AD HOC NETWORKS

To achieve security in ad hoc networks, there are existing solutions. The problems of current solutions and assumptions under their solutions introduce the necessity for the CRYPTO-AD-HOC network. These are the topics covered in this chapter.

4.1 Existing Solutions

Current suggested solutions for a secure ad hoc network fall into two categories. The first category is ad hoc routing itself in terms of security. The second category is security solutions applied for secure ad hoc networks.

4.1.1 Ad hoc Network Protocols from a Security Perspective

In contrast to traditional networks, an ad hoc network has special characteristics, such as distributed operation, dynamic network topology, fluctuating link capacity, and low power. In ad hoc networks, a routing algorithm supports mobility. On the other hand, in a mobile IP, the forwarding mechanism is used in order to support mobility. The ad hoc routing has the following characteristics: limited bandwidth environment, uncertainty of path, and random movement.

To evaluate an ad hoc network, we have to consider that an ad hoc network has special characteristics, as listed above. Furthermore, an ad hoc network needs to have a basic network functionality, such as security, efficiency, good performance by viewing the throughput and delay, query response time, minimization of control traffic, and reliability. A simulation study [2] compares two reactive routing algorithms and one
proactive routing algorithm. Among reactive routing algorithms, the Ad hoc On-demand Distance Vector and the Dynamic Source Routing were chosen for comparison. From proactive routing algorithms, the Destination-Sequenced Distance Vector is selected. From this simulation, we learn that the reactive algorithms perform better than the proactive algorithms with respect to throughput and delay. In addition, the proactive protocol does not act reliably, which means it works differently during simulation cases.

To maintain good security, low control traffic is good in terms of saving power consumption and bandwidth. With limited bandwidth, a reactive protocol is more appropriate than a proactive protocol due to saving resources to update paths. In other words, as node mobility increases, a pure proactive protocol is not appropriate because periodic control messages to maintain routes cause resources to become depleted. Even though reactive protocols cause network traffic only when the routing has to be changed, there is a delay to determine a route.

Achieving availability and avoiding Denial of Service include self-stabilization and robustness of routing. Self-stabilization is related to routing protocols themselves, such as reactive protocols, proactive protocols, and hybrid protocols. Using a centralized resource, for example, a time resource, is not a good method because of the dynamic characteristics of ad hoc networks. In addition, from the security viewpoint, the source routing method is not desirable because the routing information in packet headers is important to keep the ad hoc network secure.

4.1.2 Security Issues

Next, I look at current existing solutions for secure ad hoc networks with respect to security services: confidentiality, integrity, authentication, trust relationship, and availability. Here a trust relationship management is added as a security service because
in an ad hoc network, trust is essential. Due to an unreliable environment for an ad hoc network, we have to use cryptography in which cryptographic key management is a critical issue. In the next section, I evaluate the security service from the following viewpoints:

1. Security goal in an ad hoc network (location privacy, distributed security service, isolation, self-stabilization, and so forth),

2. Main attacker classification (insider or outsider),

3. Main relevant research area classification, and


Table 4.1 illustrates current existing solutions in terms of general security service criteria, a security goal in an ad hoc network, and main attack and attacker classification. Furthermore, my analysis of existing solutions considers the other evaluation criteria for an ad hoc network when we consider security aspects. The main relevant research area shows the focused research area on ad hoc networks. The following subsections discuss existing solutions in detail.
<table>
<thead>
<tr>
<th>General Security Service Criteria</th>
<th>Security Goal in an Ad hoc Network</th>
<th>Possible Main Attacker</th>
<th>Main Relevant Research Area</th>
<th>Current Existing Solutions</th>
</tr>
</thead>
</table>
| Confidentiality                  | • Location privacy: that is, to avoid routing information disclosure  
• However, not always desirable feature | Outsider Security       | NDM (Nondisclosure Method)  |
|                                  | • Against traffic analysis        | Outsider/Insider       | Security                    | Link-to-link encryption    |
|                                  | • Against traffic analysis        | Outsider/Insider       | Security                    | Bidirectional tunnels      |
| Integrity                        | • Avoid creation of bogus routing information  
• Avoid black hole attack         | Outsider Security       | IPSec                       |
| Authentication                   | • Avoid fabrication attack        | Outsider Security       | IPSec                       |
|                                  | • Avoid fabrication attack        | Outsider Routing Protocol | Not desirable to use source routing |
| Trust Relationship Management and Key Management | • To improve availability | Outsider Security       | A single Certificate Authority |
|                                  | • To improve availability         | Outsider/Insider Security | Replicated copies of the Certificate Authority |
|                                  | • To get availability  
• Avoid Byzantine failure by compromised node | Outsider/Insider Security | Threshold cryptography and a proactive security mechanism |
Table 4.1-Continued

<table>
<thead>
<tr>
<th>General Security Service Criteria</th>
<th>Security Goal in an Ad hoc Network</th>
<th>Possible Main Attacker</th>
<th>Main Relevant Research Area</th>
<th>Current Existing Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Relationship Management and Key Management</td>
<td>• To get availability</td>
<td>Outsider</td>
<td>Security</td>
<td>Group management by single group controller</td>
</tr>
<tr>
<td></td>
<td>• To get availability</td>
<td>Outsider/ Insider</td>
<td>Security</td>
<td>Group management by multiple group controllers</td>
</tr>
<tr>
<td></td>
<td>• To avoid Byzantine failure by compromised node</td>
<td>Insider/ Outsider</td>
<td>Security</td>
<td>Key management</td>
</tr>
<tr>
<td>Availability</td>
<td>• To get Byzantine robustness and self-stabilization</td>
<td>Insider</td>
<td>Routing</td>
<td>Redundant Paths</td>
</tr>
<tr>
<td></td>
<td>• To isolate compromised node</td>
<td>Outsider</td>
<td>Routing</td>
<td>Reactive routing protocol</td>
</tr>
<tr>
<td></td>
<td>• To get Byzantine robustness and self-stabilization</td>
<td>Outsider</td>
<td>Routing</td>
<td>Proactive routing protocol</td>
</tr>
<tr>
<td></td>
<td>• To get Byzantine robustness and self-stabilization</td>
<td>Outsider</td>
<td>Routing</td>
<td>Hybrid routing protocol</td>
</tr>
</tbody>
</table>

4.1.2.1 Confidentiality

Confidentiality assures that information is accessible only by authorized parties.

Any form of disclosure, including revealing the existence of nodes, can damage the networks. In an ad hoc network, keeping location privacy is critical. In addition, protection against traffic analysis is necessary, the same as in traditional networks.
The information in a packet header is the location of nodes or information about network topology. A routing information disclosure attack has to be prevented, but protection of location information is not always desirable. For instance, in a commercial situation, such as cellular phone services, the operator attempts to find the location of the user nodes. To avoid routing information disclosure, there is a solution to the confidentiality of location using the Nondisclosure Method (NDM).

The Nondisclosure Method for supporting location privacy protection is introduced in [3]. Independent Security Agents (SAs: each Security Agent is represented \( S_{Ai} \), where \( i \) represents sequence numbers from 1 to \( N \)) are distributed and have a pair of asymmetric cryptographic keys, that is, a public key and a private key. Each security agent knows only the mobile IP address of the previous and the next hop. The sender (S) transmits the encrypted message \( (M_{Enc}) \) by public keys \( (K_{pS_{Ai}}) \) through SAs to the receiver (R). The procedure is as follows; \( S \rightarrow S_{A_{1}} \rightarrow S_{A_{2}} \rightarrow \ldots \rightarrow S_{A_{i}} \rightarrow R \). The encrypted message \( (M_{Enc}) \) has the following format; \( M_{Enc} = E_{S_{A_{1}}}(S_{A_{2}},(E_{S_{A_{2}}}(S_{A_{3}},(\ldots((E_{S_{A_{N}}}(R,M))\ldots))))), \) in which \( E \) stands for encryption using a public key. After the \( S_{A_{1}} \) receives the \( M_{Enc} \) from the sender, the \( S_{A_{1}} \) decrypts the outmost encrypted message and forwards the packet to the \( S_{A_{2}} \). A similar process will continue until a packet arrives at the last security agent \( (S_{A_{N}}) \). At the end, the \( S_{A_{N}} \) decrypts the message and forwards it to the receiver.

Methods against traffic analysis are suggested by Fasbender et al. [15] to protect location information. For example, link-to-link encryption or bidirectional tunnels are suggested for ad hoc networks, as they are suggested for traditional networks.

4.1.2.2 Integrity

The security service called integrity makes certain that only authorized parties are able to modify transmitted information. Routing information integrity in an ad hoc
network avoids creating of bogus routing information and protects against a black hole attack. In a black hole attack, an adversary creates a reply assuming the shortest route so that it creates a forged route.

A solution exists to avoid creation of bogus routing information using the IPSec. The IPSec Authentication Header and the Encapsulating Security Payload [16, 17] are introduced for secure routing in the Ad hoc On-demand Distance Vector Routing against the creation of bogus routes. To prevent impersonation, the IPSec plays the role of authentication in the routing protocol. The sender and receiver share a pair of symmetric keys to communicate with each other. After the sender broadcasts the Routing Request message to the network, the Routing Reply message is created in the Ad hoc On-demand Distance Vector Routing with a shared key using the IPSec Authentication Header or Encapsulation Security Payload. When the Routing Request message is forwarded back to the sender, the encryption or authentication is checked and recomputed between all hops.

4.1.2.3 Authentication

The issue of correctly identified the origin of the message is related to authentication. From the authentication viewpoint, source routing, such as the Dynamic Source Routing, is not desirable because it allows the attacker to insert counterfeit objects and spoof traffic so that it causes a forged routing problem. To avoid a fabrication attack, there are solutions that use the IPSec or solutions that avoid selection of source routing. Using the IPSec in the Ad hoc On-demand Distance Vector Routing for authentication is introduced in the previous section, namely, integrity.
4.1.2.4 Trust relationship management and key management

To protect routing information and data traffic, introducing a cryptographic mechanism into an ad hoc network requires trust relationship management and key management. Trust relationship management and key management are important in terms of availability, for example, to avoid Denial of Service or to avoid Byzantine failure by a compromised node. Distributed security service is essential for key management and trust relationship management, due to the fact that if there is a centralized control and the control node is compromised, the damage is severe to the entire network. Furthermore, due to limited power, lightweight computation is needed for trust relationship and key management. Therefore, expensive computation (for instance, public key cryptography or shortest path algorithms for large networks) must narrow down the scope to a small range.

For key management, the trusted entity called a Certificate Authority is used in a public key infrastructure. In a public key infrastructure, each node has a public/private key pair. Public keys are known to others, whereas private keys must be kept securely in each node. Public key infrastructure is superior in distributing keys and achieving integrity and nonrepudiation. After the nodes authenticate each other, to establish a shared session key, a secret key scheme is used for further communication. The trusted Certificate Authority has a public and private key pair and signs certificates binding public keys to each node. Each node needs a revocation of a public key and periodically regenerate its key pair. For a trust relationship management, a revocation of a public key is necessary in case the node is no longer trusted or is out of the network. Against a brute force attack on a private key, each node refreshes its key pair periodically.
A solution exists using a single Certificate Authority for key management. In addition, replication of the Certificate Authority is used for improving availability. However, these two approaches are vulnerable to a single point attack. Therefore, Zhou and Hass [18] introduce threshold cryptography and a proactive security mechanism.

The main idea of threshold cryptography is distributing trust to a set of nodes called servers, which share the key management responsibility. In an \((n, t+1)\) threshold cryptography (where, \(n \geq 3t+1\)), \(n\) key management servers share the ability of signing the certification. The entire key management system has a public/private pair \((K/k)\). The private key \(k\) of the service is divided into \(n\) shares, which are called an \((n, t+1)\) sharing of \(k\), and assigned to each server as a form of public/private pair \((Ki/ki)\). In the \((n, t+1)\) threshold scheme, at most, \(t\) parties can be compromised. The compromised servers can generate an invalid partial signature. To defend compromised servers, a combiner works for the process of verification and construction of the correct signature with \(t+1\) correct partial signatures. Even though \(t\) servers are compromised, each of \(t+1\) parties can correctly generate a partial signature for the certificate using its private key share. After the generation of a partial signature, each of \(t+1\) parties submits the partial signature to a combiner, so that a combiner finally computes the complete signature for the certificate. Due to the joint cryptographic operation of any \(t+1\) servers, the system is resistant to compromised servers. For instance, in a \((3,2)\) threshold scheme, any one \((t=1)\) server is allowed to be compromised and even though one server is compromised, the other two \((t+1=2)\) can generate correct partial signatures so that the entire system works correctly.

In using threshold cryptography for key and trust management, all nodes in an ad hoc network know the public key of the threshold cryptographic service (\(K\)), turn in query requests to get other nodes’ public keys \((Pj)\), or submit update requests to change their
own public keys \((P_i)\). In a threshold cryptographic system, each server \((i)\) has its own key pair, that is, a public/private pair \(K_i/k_i\) and stores the public keys of all the nodes in an ad hoc network \((P)\)s. In addition, each server knows the public keys of other servers \((K_i)\).

Figure 4.1 shows key management in each server and each node in an ad hoc network and trust management to generate a signature in a threshold signature scheme.

![Diagram](image_url)

- \(K/k\): public/private key pair of the threshold service
- \(K_i/k_i\): public/private key pair in each server
- \(P_i/p_i\): public/private key pair in each node
- \(K\): public key for the entire threshold service
- \(P_i\): public key of each node
- \(K_j\): public key in other server
- \(P_j\): public key in other node
- \(m\): message
- Partial signature \(PS(m, s_i)\) using its share \(s_i\)
- \(C\): combiner
- \(\text{Fail}\): in server 2
- \((m)_k\): signature

Figure 4.1: Key management and trust management in each server and each node\(^1\)

---

\(^1\) Adapted from Zhou and Hass [18]
The other approach in dealing with trust relationship is allowing a delegation of trust [19, 20]. The approach is built on the public key approach [19]. There are three assumptions: First, trust can be delegated between nodes. Second, connectivity in the network exists between all the nodes. Third, this delegation of trust is maintained by a reactive ad hoc routing protocol. In the group, the nodes that have established trust relationships can extend trust relationship to other group members. Group membership management is suggested for ad hoc networks, in which the trust is delegated and the authority for admission and revocation of members is distributed multiple nodes [20].

4.1.2.5 Availability

Availability means the information is available only to authorized parties when needed. This security service considers the Denial of Service issue, and it is critical in an ad hoc network because of the dynamic changes in network topology. Furthermore, availability is related to self-stabilization and the robustness of routing, which means the network service is available even though there is problem in routing. A routing has to recover from any problem without human operation. In terms of availability, it is important to deal with the compromised node, key management, and the robustness of routing itself to avoid Denial of Service.

If there is a compromised node, it has to be isolated from routing and routing protocol should maintain the function correctly. In key management, if the security service is centralized, for example, replicated copy, then one compromised node causes the entire ad hoc network to crash. Therefore, security service has to be distributed. A compromised node can distort the routing, cause Byzantine failures, and propagate wrong information throughout the network. However, it is difficult to deal with the
compromised node because the node was already trusted as a member of the routing and expected to operate correctly.

To deal with a compromised node, a redundant path approach by Hass [18, 21] is based on the following assumptions. If routing protocols can find multiple paths, nodes can switch to an alternative route when the primary route has failed. Protocols such as the Dynamic Source Routing, the Ad hoc On-demand Distance Vector, the Temporally-Ordered Routing Algorithms, and the Zone Routing Protocol can discover multiple paths. Under this situation, diversity coding takes advantage of multiple paths without message retransmission. Transmitting redundant information through additional disjoint channels allows error detection and recovery.

4.2 Limitations of Existing Solutions

Even though current existing solutions try to solve the security problems in ad hoc networks, they are not enough. The following sections show the problems of ad hoc routing in terms of security and the limitations and weaknesses of existing solutions for secure ad hoc networks. These problems realize a need for CRYPTO-AD-HOC network.

4.2.1 Limitations of Existing Protocol from a Security Perspective

Availability is related with the robustness of the routing protocol itself. The reactive protocols request a route when it is needed. For example, in the Ad hoc On-demand Distance Vector, the Routing Reply message initiates routing table entries for the destination in the intermediate nodes. These entries expire after a certain amount of time. Thus, if the wrong information remains in the routing tables for a long time, it is difficult to achieve self-stabilization. On the other hand, the proactive protocols maintain routes to all nodes so that they require periodic control messages. In proactive protocols, the
attacker can send considerable routing information to cause overflow in a routing table. The routing table overflow results in preventing creation of new routes and prohibiting good communication. In addition, in a proactive protocol, if the periodic updating terms are far away from each other, an attacker can exhaust resources. The hybrid approach called the Zone Routing Protocol is desirable because the compromised part can be limited within the zone and the remaining parts can be secure.

With respect to location privacy, the Zone Routing Protocol is desirable because the zone routing information can be hidden from the outsider except communication through the Interzone Routing Protocol. In the Zone Routing Protocol, the information that the entire network has is limited because the reactive protocol, that is, the Interzone Routing protocol, is applied only when there is communication required over the zone. On the other hand, in a proactive protocol approach, the location information of the node is exposed to the entire network.

It is not desirable to use a centralized resource, for example, time resource, in a dynamic ad hoc network environment. Therefore, in terms of security, the Temporally-Ordered Routing Algorithm that use synchronized clocks for multicasting is vulnerable to attack because this algorithm depends on a time resource.

From the authentication viewpoint, the source routing method, such as the Dynamic Source Routing, is not desirable because the routing information in packet headers, that is, the location information, has the risk of information disclosure. If routing information is disclosed to the attacker, there will be changes of network topology or exhaustion of resources. If source routing is used, the adversary can cause fabrication by insertion of counterfeit objects or traffic spoofing. Table 4.2 shows the problems of existing ad hoc routing in terms of security.
Table 4.2: Lists of Limitations of Ad hoc Routing Protocols in Terms of Security

<table>
<thead>
<tr>
<th>General Security Service Criteria</th>
<th>Security Goal in an Ad hoc Network</th>
<th>Current Existing Solutions</th>
<th>Problems or Limitations of Existing Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>• Avoid fabrication attack</td>
<td>Source routing</td>
<td>• Not desirable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If used, need authentication</td>
</tr>
<tr>
<td>Availability</td>
<td>• To get Byzantine robustness and self-stabilization</td>
<td>Reactive routing protocol</td>
<td>• Possibility of difficulty in achieving self-stabilization if wrong information remains for a long time</td>
</tr>
<tr>
<td></td>
<td>• To get Byzantine robustness and self-stabilization</td>
<td>Proactive routing protocol</td>
<td>• If source routing used, possibility of fabrication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Possibility of overflow in routing table by attacker traffic analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Exposure of location information</td>
</tr>
</tbody>
</table>

4.2.2. Limitations of Existing Solutions for Security

The existing solutions for secure ad hoc networks have problems. I begin this section with an overview of existing solutions and problems, as seen in Table 4.3. I then look at each of the solutions and problems in detail. To evaluate solutions for a secure ad hoc network, we must consider the following criteria: security aspects (location privacy, distributed security service, isolation, self-stabilization, and so forth), performance (throughput and delay), power consumption by overhead (computation overhead or traffic overhead), and scalability.
Table 4.3: Lists of Limitations of Existing Solutions for Secure Ad hoc Networks

<table>
<thead>
<tr>
<th>General Security Service Criteria</th>
<th>Security Goal in an Ad hoc Network</th>
<th>Current Existing Solutions</th>
<th>Problems or Limitations of Existing Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>• Location privacy: that is, to avoid routing information disclosure. • However, not always a desirable feature</td>
<td>NDM (Nondisclosure Method)</td>
<td>• Possibility of traffic analysis • Overhead due to public key cryptography</td>
</tr>
<tr>
<td></td>
<td>• Against traffic analysis</td>
<td>Link-to-Link encryption</td>
<td>• Possibility of compromised node</td>
</tr>
<tr>
<td></td>
<td>• Against traffic analysis</td>
<td>BiDirectional tunnels</td>
<td>• Unsafe</td>
</tr>
<tr>
<td>Integrity</td>
<td>• To avoid creation of bogus routing information • Avoid black hole attack</td>
<td>IPSec</td>
<td>• Overhead due to key distribution</td>
</tr>
<tr>
<td>Authentication</td>
<td>• To avoid fabrication attack</td>
<td>IPSec</td>
<td>• Overhead due to key distribution</td>
</tr>
<tr>
<td></td>
<td>• To avoid fabrication attack</td>
<td>Source routing</td>
<td>• Not desirable</td>
</tr>
<tr>
<td>Trust Relationship Management and Key Management</td>
<td>• To improve availability</td>
<td>A single Certification Authority</td>
<td>• Problem in availability due to vulnerability to a single point attack • Collapse of the secure communication • Impersonation of node or revocation of certificate</td>
</tr>
<tr>
<td></td>
<td>• To improve availability</td>
<td>Replicated copies of the Certificate Authority</td>
<td>• Vulnerability to a single point attack</td>
</tr>
<tr>
<td>General Security Service Criteria</td>
<td>Security Goal in an Ad hoc Network</td>
<td>Current Existing Solutions</td>
<td>Problems or Limitations of Existing Solutions</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td><strong>Trust Relationship Management and Key Management</strong></td>
<td>• To get availability • Avoid Byzantine Failure by compromised node</td>
<td>Threshold cryptography and proactive security mechanism</td>
<td>• Cause Denial of Service • Problem in availability • Computational overhead • Slow decision-making</td>
</tr>
<tr>
<td></td>
<td>• To get availability</td>
<td>Group management by single group controller</td>
<td>• Vulnerability to a single point attack</td>
</tr>
<tr>
<td></td>
<td>• To get availability • Avoid Byzantine Failure by compromised node</td>
<td>Group management by multiple group controller</td>
<td>• Problem in keeping track of entire group management</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>• To get Byzantine robustness and self-stabilization • Require to isolate compromised node • Require to distribute security service</td>
<td>Key management</td>
<td>• Avoid Power consumption overhead</td>
</tr>
<tr>
<td></td>
<td>• To get Byzantine robustness and self-stabilization • To isolate compromised node</td>
<td>Redundant paths</td>
<td>• Limited detection • High cost • Overhead in computation and network traffic</td>
</tr>
</tbody>
</table>
4.2.2.1 Limitations of confidentiality techniques

The Nondisclosure Method for supporting location privacy protection contains problems. The overhead is introduced because of public key cryptograpy. The sender needs to know all the public keys and the security agents in the route to construct the route. In addition, if payloads of packets are not padded with random data, then it is possible for the attacker or compromised node to do traffic analysis based on packet length.

The other form of avoiding location information disclosure is against traffic analysis, such as link-to-link encryption and bidirectional tunnels [15]. Link-to-link encryption is scalable in key management. However, this approach has limitations. By handling decrypted data in plaintext form, link-to-link encryption has the possibility of causing compromised nodes. On the other hand, a bidirectional tunnel is not secure due to the characteristics of the tunnel, which is observable and does not always exist in an ad hoc situation.

4.2.2.2 Limitations of integrity assurance techniques

To avoid creation of bogus routing, that is, to keep integrity in routing information, applying the IPSec has the following drawbacks. If the IPSec is applied to the Ad hoc On-demand Distance Vector, then after the Routing Reply message is sent by the receiver the attacker can intercept the message. Despite the IPSec encryption or authentication, the attacker therefore can create a bogus route, if the malicious message arrives to the sender before the correct message. Also, this protection cannot work successfully if any of the trusted nodes that want to communicate are compromised. The last limitation is that this approach causes overhead due to key distribution.
4.2.2.3 Limitations of authentication mechanisms

Applying the IPSec authentication creates problems, as shown in the integrity section. Using source routing, such as the Dynamic Source Routing, is not desirable in terms of authentication. If source routing is used for ad hoc networks, an authentication process is needed for secure routing. This authentication causes overhead, especially when public key cryptography is used.

4.2.2.4 Limitations of key and trust relationship management mechanisms

Key management and trust relationship management are important to secure the entire network and establish secure communication in terms of availability. In managing key and trust relationships, it is important to distribute security service and make lightweight computation.

For key management, using a Certificate Authority or using replication of a Certificate Authority contains problems. Using a single trusted entity called a Certificate Authority in a public key infrastructure can cause serious problems in terms of availability. If a Certificate Authority is not available, nodes cannot get the current public keys of other nodes, which results in the collapse of secure communication. If a Certificate Authority is compromised and leaks its private key to an attacker, the attacker can sign a wrong certificate using a Certificate Authority’s private key, which leads to the impersonation of the node or revocation of the certificate. In using a replication of a Certificate Authority, compromise of any replica that has the private key can introduce serious vulnerability.

Using threshold cryptography and a proactive security mechanism for trust management and key management [18] creates problems. Applying threshold cryptography for trust management has limitations because of certain assumptions and
conditions. Among the assumptions and conditions, the following facts are necessary for evaluation. At most, \( t \) servers can be compromised in any period of time for a certain duration, and the private key of the service is never disclosed to an attacker. However, it is possible for servers to be compromised more than \( t \) servers, and the private key of service can be exposed so that proactive threshold cryptography is suggested. In a proactive scheme, share refreshing is used for servers to compute new shares from old ones without disclosure of the private key to any server. However, applying threshold cryptography and a proactive scheme still contains problems. Threshold trust management is suggested to improve availability, that is, to avoid Byzantine failure by one single centralized Certificate Authority. Threshold schemes, however, can result in reducing availability because of the Denial of Service. In a threshold scheme, the combiner has a verification process of a threshold signature after obtaining correct partial signatures from any \( t+1 \) servers. Therefore, the threshold scheme causes considerable computational overhead and slow decision-making.

Applying delegation of trust [19, 20] for trust management contains the following problems. In a single group controller approach, if a centralized group controller is compromised, a group cannot be managed properly. However, a solution using multiple group controllers also has problems. There is no way to keep track of an entire group management, and redundant certification makes trust management complicated.

4.2.2.5 Limitations of availability mechanisms

To achieve route robustness by dealing with a compromised node, Hass [18, 21] assumes redundant paths, that is, multiple routes. This redundancy allows the entire network to operate consistently even though there are compromised nodes. However, multiple routes can create high costs and overhead in computation, which come from the
following assumption: Given the overhead factor, the diversity coding has advantages of reducing transmission delay in comparison with retransmission of the packet. More seriously, the redundant route approach is restricted because the route endpoints, which are necessary to switch to another route, cannot always detect an attack.
CHAPTER 5
PROPOSED APPROACH: THE CRYPTO-AD-HOC NETWORK

In Chapter 5, I introduce the CRYPTO-AD-HOC network as a novel, and discuss its importance and protocol design. The protocol design of the CRYPTO-AD-HOC network includes the following features: overall architecture, key management and trust relationship management, authentication and confidentiality mechanism, availability mechanism, security level, and ad hoc routing.

5.1 Overview of the CRYPTO-AD-HOC Network

The CRYPTO-AD-HOC network is based on a hybrid ad hoc solution, namely the Zone Routing Protocol [4]. The Zone Routing Protocol consists of two major protocols, the Intrazone Routing Protocol and the Interzone Routing Protocol.

The main security challenge of ad hoc networks is related to key management and trust relationship management. Key management adopts the Public Key Infrastructure, which is superior to distribution of keys and achievement of integrity. For trust relationship management, I used the concept of a flexible bottom-up trust model so that no single composed key causes critical reconfiguration problems. I call this process Trust Relationship Management Process (TRMP). For authentication, I use a digital signature and message digest, which will henceforth be called the Digital Signature and Message Digest Process (DSMDP). After authentication, establishing a shared secret session key is used to secure communication.
For achieving confidentiality, I encrypt actual data, as well as header information, to protect the IP address information using a Rivest-Shamir-Adelman (RSA) algorithm. The process is called Encryption Process (ENCP). For availability, detection of intrusion or compromised node is necessary. I call this process the Intrusion or Compromised Node Detection Protocol (ICNDP), which cooperates with the Neighbor Discovery and Maintenance Protocol. The Neighbor Discovery/Maintenance Protocol is not specified but assumed in the Zone Routing Protocol.

Furthermore, setting the different security levels according to the users’ needs means that the entire protocol has diverse security features. The security level is set in protection level, but the detection level is assumed. The reaction level is currently out of scope of this thesis even though that level is necessary. In the protection level, encryption takes four ranks: no encryption, encryption of actual data and IP address information, encryption only of actual data, and encryption of IP address information. The detection level includes intrusion or compromised node detection, except intrusion tolerance.

Figure 5.1 shows the overview of the entire process of message delivery from sender node to destination node with respect to each common node and Certificate Authorities regarding the routing and security consideration, that is, trust relationship management, key management, authentication, and intrusion and compromised node detection, and different level of encryption for confidentiality.
Figure 5.1: Overview of the CRYPTO-AD-HOC network in terms of route discovery and security aspects: trust relationship management, key management, encryption, and authentication. Intrusion or compromised node detection is assumed.

Figure 5.2 illustrates the overall picture of the CRYPTO-AD-HOC network to explain routing in the Zone Routing Protocol, authentication, trust relationship management, and key management regarding Certificate Authorities and common nodes that participate in routing.
5.2 Importance of the CRYPTO-AD-HOC Network

The desire to achieve security more in the ad hoc network realizes a need for the CRYPTO-AD-HOC network. The CRYPTO-AD-HOC network offers a diverse security level, which aids users in communicating using the ad hoc network in a secure way. The
CRYPTO-AD-HOC network enhances security aspects and empowers the ad hoc network study by supporting a creation of realistic security models.

The main ideas of the CRYPTO-AD-HOC network are accommodated to mobile ad hoc network characteristics and achieve the requirements for a secure ad hoc network, for example, lightweight computation, location privacy, and verification of discovered routes by protecting the location address itself. In terms of security features, the goals of the CRYPTO-AD-HOC network are not only to prevent routes from attack or misbehaving nodes but also to detect and isolate compromised nodes.

5.3 Design of the CRYPTO-AD-HOC Network

The CRYPTO-AD-HOC network focuses on ad hoc networking to be performed appropriately adding security aspects under different realistic situations, such as military situations, rescue or emergency, and home networks. The protocol implements the security characteristic of ad hoc networks by setting different security levels. Security levels are application-dependent. Details on protocol design are given in the following subsections: design assumptions, key management and trust relationship management, authentication mechanism, confidentiality mechanism (including protection of IP address information), availability mechanism (detection mechanism), applying different security levels (protection and detection level), and routing.

5.3.1 Design Assumptions

I restrict this study to IP-based networks. For trust relationship management, I make the following assumptions. First, there is a hierarchical namespace directory so that any name can be found. Second, the name is subordinated. Third, in the namespace there
are several Certificate Authorities that compose a flexible bottom-up trust model so that peer-to-peer cross-certification is allowed.

5.3.2 Overall Architecture and Components

The Intrazone Routing Protocol and the Interzone Routing Protocol are implemented for zone routing [4]. The Intrazone Routing Protocol maintains routes within a zone, whereas the Interzone Routing Protocol discovers routes between nodes over a zone. Information is passed from the Intrazone Routing Protocol to the Interzone Routing Protocol whenever there is a request for a longer new route between nodes than the zone radius.

Key management of CRYPTO-AD-HOC network is based on the Public Key Infrastructure. The nodes in ad hoc networks are categorized two ways: special nodes called Certificate Authorities which have responsibility for establishing a trust relationship, and common nodes called principals which participate in communication. To communicate with other nodes, each common node has a private/public key pair. The Certificate Authorities usually certify each other when key pairs in common nodes are first created. The function of managing trust relationship is implemented and called the Trust Relationship Management Process. The main purpose of this process is certification generation, certification revocation, and certification distribution. This process provides a public key for verification of other nodes, which is a necessary step for authentication. At first, a trust relationship among Certificate Authorities has to be established before using certificates. Therefore, after each node generates a private/public key pair, it subscribes to a Certificate Authority close to it in the hierarchy. After Certificate Authorities generate certification for each node, the authentication process, called the Digital Signature and
Message Digest Process, is possible. In other words, the Trust Relationship Management Process works for the authentication process.

Furthermore, the function of detection of malicious behavior of other nodes is assumed. This detection, called the Intrusion or Compromised Node Detection Protocol, is supposed to work for the Trust Relationship Management Process and the Neighbor Discovery/Maintenance Protocol.

![Overall architecture of the CRYPTO-AD-HOC network](image)

- DSMDP: Digital Signature and Message Digest Process
- TRMP: Trust Relationship Management Process
- ICNDP: Intrusion or Compromised Node Detection Protocol
- ENCP: Encryption Process
- IARP: Intrazone Routing Protocol
- IERP: Interzone Routing Protocol
- NDMP: Neighbor Discovery/Maintenance Protocol
- ICMP: Internet Control Message Protocol
- IP: Internet Protocol

Figure 5.3: Overall architecture of the CRYPTO-AD-HOC network
After detection checking by the Intrusion or Compromised Node Detection Protocol, the Trust Relationship Management Process and the authentication process called the Digital Signature and Message Digest Process are running to authenticate each node to other nodes and verify other nodes. After having a trust relationship, authenticating each other, and setting a route, the packet will be delivered to its destination by the encryption mechanism, that is, the Encryption Process. The overall architecture is shown in Figure 5.3.

5.3.3 Authentication Mechanism

The Digital Signature and Message Digest Process is used for authentication. The authentication process is done after the Trust Relationship Management Process. To authenticate each other, it is necessary to verify the correspondent using correspondent’s public key. That public key can be obtained securely through a trust relationship that is detailed in the next section.

To perform an effective and secure digital signature, several procedures are introduced, for example, using a single trusted third party called a Certificate Authority, using a shared secret key, or dealing with a group key, which is the subject of the next section. Each solution is also related with key management and trust management. In addition, each solution contains different drawbacks from the viewpoint of computations and costs, performance, and risk of secret disclosure. For instance, using a shared secret key contains more risk, and a group key management case creates more overhead.

The Digital Signature and Message Digest Process is a better approach than a simple digital signature using a public key operation to authenticate each node: A simple digital signature causes expensive computation for large messages. Furthermore, the Digital Signature and Message Digest Process is better than simply using the IPSec,
because applying the IPSec has limitations: overhead due to key distribution and possibility of interception of a message by an attacker allowing the creation of a bogus route.

5.3.4 Key Management and Trust Relationship Management

Key management and trust relationship management are more important and essential than other security characteristics because ad hoc networks do not guarantee a secure environment. In the CRYPTO-AD-HOC network, a Public Key Infrastructure is adopted to achieve integrity. In addition, a public key approach is easy to distribute keys and safer than a private key approach. In a Public Key Infrastructure, trust management is the main issue to determine success of key management.

5.3.4.1 Key management

In key management, the Public Key Infrastructure is used to accomplish integrity and safety in distributing keys. Each node in an ad hoc network needs to authenticate itself and verify the identity of another node. Thus, each node has a private/public key pair. In each node, the private/public key pair is revoked periodically for the security reasons. After authentication, establishing a shared secret session key is used to secure communication.

To verify the identity of another node in the public authentication process, each node has to know the public key of another node. To support secure exchanging of public keys with each other in communication, there are special nodes, called Certificate Authorities. To provide verification, Certificate Authorities have a responsibility to generate public key certificates, which is described in the next subsection, namely, trust relationship management.
It is beneficial to change the zone radius to achieve lightweight computation, according to the situations. The reason to change the zone radius is that the key distribution is accompanied by computation, and lightweight computation is a critical point in an ad hoc network that consists of mobile nodes.

Trust management based on the Public Key Infrastructure is better than a group membership approach. In a group membership approach, the distribution of group keys is also a problem, and it creates considerable overhead for the entire network.

5.3.4.2 Trust relationship management

The Trust Relationship Management Process runs to set and manage the trust relationship in an ad hoc network. It is important for each node to establish trust before it communicates with each other. For the Trust Relationship Management Process, there are trusted nodes known as Certificate Authorities that digitally sign data structures, namely, certificates.

The trust model I use is the flexible bottom-up trust model for certification. To establish this trust model, I have made the following five assumptions. First, there is a hierarchical namespace directory so that any name can be found. Second, the name is subordinated. Third, in the namespace, there are Certificate Authorities that compose a flexible bottom-up trust model allowing peer-to-peer cross certification. Fourth, at least two Certificate Authorities exist on top of the trust model expressing peer-to-peer certificates. Fifth, trust delegation is application-dependent and should be restricted by policy.

In the flexible bottom up trust model, each Certificate Authority owns three types of certificates, such as down, up, and cross certificates. The down certificate means a parent certifies the key of the child, whereas the up certificate means a child certifies the
key of the parent. The cross certification means any one can certify the key of any other. In the bottom-up model, the ancestor is the least common ancestor, which means there is the common prefix in names. This flexible bottom-up model has two important benefits. First, no single compromised key causes massive reconfiguration in the entire network. Second, in an ad hoc network, users are not necessary to traverse several layers of hierarchy to reach a certificate authority.

Before the use of certificates, Certificate Authorities establish a trust relationship with each other. Figure 5.4 provides examples of certification among Certificate Authorities in a flexible bottom-up trust model. In examples 1 and 2, as I mentioned already as an assumption of this thesis, there are two top autonomous Certificate Authorities which are connected with a peer-to-peer cross certificate, for instance, top1 and top2, as well as top3 and top4. Therefore, even though the key of top1 is compromised, the entire network does not need reconfiguration.

![Figure 5.4: Example of trust relationship among Certificate Authorities in a flexible bottom-up trust model](image-url)
Figure 5.5 shows an example of certification links among Certificate Authorities and common nodes in namespace hierarchy as an extension of example 1 in Figure 5.4. The following sentences list which Certificate Authorities certify which node in Figure 5.5: top1 certifies top2, low1, n1, and n2. Top2 certifies top1, mid1, mid2, and n6. Mid1 certifies top2, n7, n8, and n9. Mid2 certifies top2, n10, and n11. Low1 certifies top1, n3, n4, and n5.

Figure 5.6 shows an example of a necessary certification from source to destination node regarding Certificate Authorities and common nodes in namespace hierarchy as an extension of example 2 in Figure 5.4. In this example, if n7 is a source and n6 is a destination, n7 has to trust only low2 and mid3.
Cross certification is established between two Certificate Authorities by the signing of one Certificate Authority’s public key for another. An autonomous Certificate Authority can establish peer-to-peer cross certification with another autonomous Certificate Authority. This provides flexibility and great benefit: If one Certificate Authority is compromised, it does not cause massive reconfiguration. In this thesis, therefore, assume that at least two autonomous Certificate Authorities are on top.

To establish a bottom-up trust model, in addition to namespace, other trust constraints, such as path length, name, and policy constraint, are required. These constraints are included in the X.509 version 3 standard as an extension. In my scheme, however, these are requirements for establishing a trust model, and these are applied differently, depending on the application of ad hoc networks. By path length constraints,
a Certificate Authority can control trust delegation, for example, the path length constraint is equal to one. By name constraints, a trust is limited to a certain subgroup of another Certificate Authority, for instance, a specific department of rescue and emergency. By specifying policy constraints, a trust is restricted to a certain group with policy value, for example, highly classified users in the military.

The certificate is important with respect to expiration of authentication, that is, authentication is still valid as long as the certificate is valid. However, authentication is useful during the typical session. Trust delegation, in which a surrogate acts for the original Certificate Authority, should be limited to a specific desirable situation because it is application-dependent, for example, military circumstances. Therefore, to delegate trust, policy or specification of groups can be used. To minimize the damage of compromise, if the delegation is no longer honorable, then it is necessary to revoke nodes in a lower hierarchy.

Trust revocation should be necessary in cases when the key is compromised, when the certification is compromised, or when a certain Certificate Authority no longer trusts a node. Each Certificate Authority has to maintain a Certificate Revocation List (CRL) for all revoked certificates by that Certificate Authority and post it to well-known places called directories. Whenever a node receives a certificate to get a public key, it must check to see if the certificate is still valid. For reliability, if each node caches a certificate, it should periodically check to see if the cache is still valid.

Trust relationship management, that is, a flexible bottom-up trust model using several Certificate Authorities and peer-to-peer cross certification, is better than using other schemes, for example, using the only single Certificate Authority. Dealing with
command nodes and control nodes is crucial in ad hoc networks because they have important roles to perform over the entire network. If command nodes or control nodes are compromised, the damage is more serious than common nodes. In a single Certificate Authority approach, the Certificate Authority is responsible for revocation of nodes that are no longer trusted. Therefore, the single Certificate Authority is highly vulnerable to attack. Whoever stole the Certificate Authority’s private key can generate bogus certificates. As a result, it is possible for one person to impersonate another person.

Furthermore, trust relationship management is better than threshold cryptography because it can reduce considerable computation overhead that exists in a threshold cryptography scheme. Moreover, this approach is more secure than applying a trust delegation concept into a reactive ad hoc routing protocol. A trust delegation can cause a malicious node to be installed, and the compromise may go for a significant period of time. Besides, applying a trust delegation to a reactive routing uses a flooding method so that it is not a scalable approach if the entire network has many nodes.

5.3.5 Confidentiality Mechanism

A data packet delivered through the CRYPTO-AD-HOC network is encrypted using the RSA scheme. In an ad hoc network situation, in some cases the location, that is, the IP address information, is more valuable than the actual delivered data. Therefore, the header of the packet that has the location information is also encrypted so that the location information is verified.

5.3.6 Availability Mechanism

Availability is related with routing robustness. To increase availability, the intrusion detection and reaction mechanism are necessary. The security service can be classified along the time line: prevention, detection, and reaction. The prevention
mechanism happens before the attack and includes authentication, authorization, and accounting. On the other hand, the detection mechanism happens during the attack. The reaction mechanism takes place after the attack and includes the attack assessment, damage assessment, and data recovery.

5.3.6.1 Intrusion detection mechanism

The detection mechanism happens during the attack. The target area of the detection mechanism is the intrusion detection, compromised node detection, and intrusion tolerance, so that these issues are highly related with the robustness of routing, as well as availability. The Intrusion or Compromised Node Detection Protocol is the protocol that detects the intrusion or compromised node in an ad hoc network to guarantee the trust relationship establishment and routing robustness. Therefore, the Intrusion or Compromised Node Detection Protocol works for the Trust Relationship Management Process and the Neighbor Discovery/Maintenance Protocol.

In this thesis, the Intrusion or Compromised Node Detection Protocol remains unspecified. However, the following concepts have to be assumed. The Intrusion or Compromised Node Detection Protocol communicates with the Trust Relationship Management Process to indicate there is a compromised key. In addition, the Intrusion or Compromised Node Detection Protocol works for the Neighbor Discovery/Maintenance Protocol to let it know there is an intrusion or compromised node. The Neighbor Discovery/Maintenance Protocol in the Zone Routing Protocol thus tries to repair the route and by-pass the failed connection. The Intrusion or Compromised Node Detection Protocol working with the Neighbor Discovery/Maintenance Protocol is more realistic than using a redundant path, that is, multiple routes, against a compromised node. Using a redundant path has a limitation of high cost and overhead in computation due to the
following assumption: Given the overhead factor, the diversity coding has advantages compared with the retransmission of the packet in terms of reducing transmission delay.

5.3.7 Security Level

In an ad hoc network, the security requirement must have several security levels. In terms of protection, authentication is necessary to prevent forging or modifying data, as mentioned in the previous section. To perform encryption, I set four modes: no encryption, encryption of all data and IP address information, encryption of only data, and encryption of only the IP address. The detection level involves an intrusion detection, which, assumed in this thesis and remains unspecified in details, is a basic requirement for establishing a trust relationship and robust route.

Deciding on the security level depends on several factors, such as a variety of applications, the role of nodes, and response to diversity of attacks. Regarding the levels of security and types of applications, drawing down the security requirement level in a line, the military application will rise to a higher level, emergency and rescue to a middle level, and home network to a lower level.

In the passive attacks, information, such as the location of nodes and the role of nodes, is exposed to attackers. On the other hand, active attacks make the network temporarily disabled. The security level in a protocol can be categorized in three classes: protection, detection, and reaction. Therefore, applying the security level in a protocol according to the security requirement level in applications, such as military, emergency and rescue, and home network, makes a protocol more realistic and applicable. For example, in a commercial situation, a location disclosure to an operator is sometimes a necessary feature.
5.3.8 Routing
The CRYPTO-AD-HOC network is based on the Zone Routing Protocol [4] because the Zone Routing Protocol is good in terms of security and the Reconfigurable Wireless Networks environment. The Reconfigurable Wireless Networks environment is characterized by increased mobility, a larger number of nodes, and large network span. Using the Zone Routing Protocol reduces the frequent updating cost to a constantly changing network topology. From the security viewpoint, routing information can be hidden within the zones, and exposure of the entire network information can be restricted. The Zone Routing Protocol includes the Intrazone Routing Protocol within a routing zone and Interzone Routing Protocol over a routing zone.

5.3.8.1 Routing discovery
The source node tries to find out whether or not the destination is within its routing zone. If the path to the destination exists, the route discovery process stops. If not, the source bordercasts a route query to all its peripheral nodes. Bordercasting is a form of multicasting that directs messages from one node to its peripheral nodes. This process continues until it reaches its destination. During the routing discovery process, the Intrusion or Compromised Node Detection Protocol runs.

5.3.8.2 Routing accumulation procedure
To accomplish the route discovery, source routing is needed. In source routing, a node appends its own IP address to a received query packet. Thus, the sequence of IP addresses indicates a route from the query’s source to the current node. The reverse of this sequence specifies a route back to the source. If there is sufficient storage space, caching routing information reduces query traffic and query response time. It is important to run the Encryption Process to protect the IP address information if it is required, except...
in the case of the requirement of routing information disclosure, for example, finding the user’s current locations in cellular phone service.

### 5.3.8.3 Query control mechanisms and route maintenance

To avoid a redundant query process to a previously queried node, the query source is recorded in a Detected Queries Table. Monitoring the discovered routes and repairing failed routes are needed for route maintenance. After detection of a route failure, it is necessary to notify the route’s source of the failure and/or attempt to repair the route.
CHAPTER 6
CONCLUSIONS AND FUTURE RESEARCH

6.1 Conclusions

This thesis focuses on suggesting new solutions for a secure ad hoc network. I have designed the CRYPTO-AD-HOC network to complement existing ad hoc network protocols. This new protocol enhances the security aspects, and, at the same time, the new protocol must not jeopardize performance. In addition, one of the main purposes of this thesis is to establish the criteria of evaluating security for an ad hoc network.

In this thesis, I consider an ad hoc network from the security viewpoint. At first, existing ad hoc network routing protocols are reviewed in terms of security, cost, and performance. In addition, I illustrate the goal of security service, security issues introduced by mobility, vulnerabilities and attacks in an ad hoc network, requirements for a secure ad hoc network, and some cryptographic techniques. To suggest new solutions, I analyze the existing solutions for secure ad hoc networks and note some of their problems.

In order to establish a secure ad hoc network, key management, especially trust relationship management, is essential and critical. For key management, I adopt a public key infrastructure. I propose to use a flexible bottom-up trust model using three certificate constraints types, such as path length constraints, name constraints, and policy constraints. At least two autonomous Certificate Authorities have peer-to-peer cross certifications on top of a trust relationship structure, which provides more flexibility and
reliability. As a result, the CRYPTO-AD-HOC network provides security features to users of an ad hoc network with low cost and less computation and network overhead. In the CRYPTO-AD-HOC network, users can handle the malicious intention by isolating a node that is no longer trusted.

The following functional security requirements are used as evaluation criteria: confidentiality, integrity, authentication, secure key management and trust relationship management, and availability. Wireless networks are known to have a much higher latency and bit error rate than wired networks. For performance evaluation, throughput (bytes/sec), delay (ms), and total loss (%) can be chosen as measurement factors. The lowest loss, minimum delay, and highest throughput are desirable. With performance factors, the efficiency, lightweight computation or traffic, and low cost must be taken into account. It is necessary to consider security tradeoffs, that is, convenience and availability.

The CRYPTO-AD-HOC network achieves confidentiality by protecting IP address information, as well as by avoiding traffic analysis. The public key infrastructure and trust relationship management achieve authentication and integrity, including avoiding a creation of bogus routing information and avoiding a black hole attack. Due to adopting peer-to-peer cross certification in a flexible bottom-up trust model, the computation overhead is not serious. Availability, including Byzantine robustness, is related to the routing protocol and key management. Achieving self-stabilization and isolating compromised nodes have limitations: Intrusion detection is assumed, and a reaction mechanism is not specified. Regarding convenience, requesting in-depth security levels makes this network slightly inconvenient for the user, however, this cryptographic
scheme-embedded network has better security features. Table 7.1 shows the evaluation of CRYPTO-AD-HOC network.

Table 7.1: CRYPTO-AD-HOC Network Evaluation

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Location privacy</td>
<td>IP address encryption</td>
<td>At IP level a packet header to be handled</td>
</tr>
<tr>
<td>Integrity</td>
<td>To avoid creation of bogus routing</td>
<td>Public Key Infrastructure</td>
<td>Superior to a secret key approach in terms of key distribution</td>
</tr>
<tr>
<td>Authentication</td>
<td>To avoid fabrication attack</td>
<td>Public Key Infrastructure</td>
<td>Superior to a secret key approach in terms of key distribution</td>
</tr>
<tr>
<td>Trust Relationship Management and Key Management</td>
<td>For Authentication • To get availability • To Avoid Byzantine failure by compromised node</td>
<td>Flexible-bottom-up trust model using Several Certificate Authorities • Cross Certification • Peer-to-peer certification</td>
<td>Superior to hierarchical trust model • Name servers or directories might be compromised • Performance evaluation is necessary</td>
</tr>
<tr>
<td>Availability</td>
<td>To get Byzantine robustness and self-stabilization</td>
<td>Assumes Intrusion or Compromised Node Detection Protocol</td>
<td>Intrusion or Compromised Node Detection needs to be described in detail</td>
</tr>
</tbody>
</table>

6.2 Future Research

More research is necessary to apply security mechanisms in an ad hoc network. In addition, it is difficult to deploy a unique solution because a security solution and choice
of a proper protocol are highly dependent on situations. Adding security mechanisms is necessary to investigate the impact on network performance. In this thesis, a trust relationship management depends on identity-based certificates so it might be difficult and complex to use a globally unique name. Another weakness comes from the compromise of name servers or directories. In that case, revocation cannot work and an obtained certificate can become invalid.

In this thesis, the Intrusion or Compromised Node Detection Protocol is assumed but remains unspecified. Intrusion or compromised node detection in an ad hoc network is an emerging research area, and this area is difficult topic because of ad hoc network characteristics. However, it is a crucial problem and must be solved. Besides, intrusion tolerance and reaction mechanisms have to be achieved. The reaction level deals with attack access, damage access, and data recovery. The case of recovery is related to self-stabilization, and it is the highest mechanism in dealing with security. These detection and reaction mechanisms can work with a route maintenance mechanism, that is, detection of a route failure and repair of the route.
APPENDIX
ACRONYMS

AH Authentication Header
AODV Ad hoc On-demand Distance Vector Routing
DoS Denial of Service
DSA Digital Signature Algorithm
DSR Dynamic Source Routing
EAP Extensible Authentication Protocol
EAPOL EAP over LAN
ESP Encapsulating Security Payload
IARP Intrazone Routing Protocol
IEEE Institute of Electrical and Electronics Engineers
IERP Interzone Routing Protocol
IP Internet Protocol
IP-based Internet Protocol-based
IPSec IP Security
Ipv4 Internet Protocol Version 4
Ipv6 Internet Protocol Version 6
ISAKMP Internet Security Association and Key Management Protocol
LAN Local Area Network
MAC Message Authentication Code
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MANET</td>
<td>Mobile Ad hoc Networks</td>
</tr>
<tr>
<td>MD</td>
<td>Message Digest</td>
</tr>
<tr>
<td>MIME</td>
<td>Multipurpose Internet Mail Extension</td>
</tr>
<tr>
<td>NDM</td>
<td>Nondisclosure Method</td>
</tr>
<tr>
<td>NDMP</td>
<td>Neighbor Discovery/Maintenance Protocol</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>PDAs</td>
<td>Personal Data Appliances/Assistants</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RSA</td>
<td>Rovest-shamir-Adelman</td>
</tr>
<tr>
<td>RWN</td>
<td>Reconfigurable Wireless Network</td>
</tr>
<tr>
<td>SET</td>
<td>Secure Electronic Transaction</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure MIME</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TORA</td>
<td>Temporally-Ordered Routing Algorithm</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless Personal Area Network</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WRP</td>
<td>Wireless Routing Protocol</td>
</tr>
</tbody>
</table>
WTLS  Wireless Transport Layer Security

WWAN  Wireless Wide Area Network

ZRP   Zone Routing Protocol
LIST OF REFERENCES


BIOGRAPHICAL SKETCH

Kyungjoo Suh was born on June 27, 1969, in Seoul, Korea. She received her Bachelor of Science degree in horticulture science, minoring in computer science, from Korea University, Seoul, Korea, in February 1993. In 1991, she won a prize from the 16th National Thesis Competition that is offered by the Korean Research Foundation and sponsored by the Korean Ministry of Education.

She continued her studies at Seoul National University, Seoul, Korea, and earned her Master of Science degree in landscape architecture in February 1996. Her thesis was titled: “A Study on the Analysis of the Impact of Human Activity on Sorak National Park Vegetation using Geographic Information System (GIS) and Remote Sensing Technologies.” Her specific area included GIS and remote sensing image interpretation. As a research assistant, she became involved in a national project to protect natural forest resources. In 1995, she won a prize in a thesis contest sponsored by Chosun Daily News and the Korean Land Development Corporation. As a student in Korea, she received fellowships and scholarships from Korea University as well as from Seoul National University.

Since 1996, Kyungjoo Suh had worked as a researcher and engineer as part of a solution development team at Samsung SDS Co., Ltd., Seoul, Korea. She conducted research as a systems analyst, designer, and programmer, in the Image Processing Project, which is a national research project. She conducted research on distributed multimedia database systems, the Geographic Information System, and remote sensing
technology because the Image Processing Project is a Web-based distributed database and handles nontraditional data, such as large remote sensing images, GIS spatial data, multimedia data, as well as traditional data. During this period, she realized the importance of security and mobile computing, and since that time, this subject has preoccupied her research.

She entered the University of Florida in Gainesville in the spring of 2000 and started to pursue a Master of Science degree in the Computer and Information Science and Engineering Department. She conducted research in security in ad hoc networks as a research assistant. Her research interests include security, ad hoc network and Mobile IP, mobile and wireless networks, and mobile computing.