Securing geographic routing in mobile ad hoc networks

Zhou, Zhi

2007

Zhou, Z. (2007). Securing geographic routing in mobile ad hoc networks. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/35748>

<https://doi.org/10.32657/10356/35748>

Securing Geographic Routing in Mobile Ad Hoc Networks

Zhou Zhi

School of Computer Engineering

A thesis submitted to the Nanyang Technological University
in fulfillment of the requirement for the degree of
Doctor of Philosophy

2007

Acknowledgments

I wish to express my sincere appreciations to my supervisor, Associate Professor Yow Kin Choong, for his patient assistance in my research as well as for being thoughtful and helpful all the way in some of my financial situations. My appreciation cannot be forgotten to Dr. Sukumar Nandi, whose patience, suggestions and discussions benefited me a lot and brought me into the security world when I was just starting the research.

In addition, special thanks to Huiqing for his sharing of experience with the Network Simulator-2, which was fairly helpful during the initial implementation phase of this undertaking, and Yue Xue, the author of DLM, whose prompt replies to my questions really helped a lot. Many thanks also to the members of the MANET group and my labmates for their valuable discussions.

Finally, I wish to express my deepest gratitude to my parents and my girlfriend, Xiaoxi, for their unfailing love, support and understanding when the personal pursuit drove us oceans apart for years.

Contents

Acknowledgments	i
Abstract	vii
List of Publications	ix
List of Figures	x
List of Tables	xiii
1 Introduction	1
1.1 Background	1
1.2 Mobile Ad Hoc Network Security	3
1.2.1 MANET Applications	3
1.2.2 Security Concerns	5
1.2.3 Security Requirements	6
1.3 Contributions of the Work	8
1.4 Organization of the Thesis	10
2 Related Works	11
2.1 Attacker Model	11
2.2 Types of Attacks in MANETs	12
2.2.1 Elements of Routing Attacks	13
2.2.2 Sophisticated Attacks	15
2.3 Security Schemes for Ad Hoc Routing	18
2.3.1 Ariadne	18
2.3.2 ARAN	20
2.3.3 Others	21
2.4 Cooperation for Ad Hoc Networks	24

2.4.1	Watchdog and Pathrater	24
2.4.2	Other approaches	26
2.5	Security Association Establishment	27
2.6	Summary	30
3	A Comprehensive Study of Geographic Routing Security	33
3.1	Overview of Location-based Routing	34
3.1.1	Forwarding Strategies	34
3.1.2	Location Services	36
3.2	Attacks on Geographic Routing	38
3.2.1	Analysis of cooperation	38
3.2.2	Forwarding misbehavior	39
3.2.3	Malicious attacks	42
3.2.4	Attacks on location service	45
3.3	Countermeasures	47
3.3.1	Authentication: external attack prevention	47
3.3.2	Post-Authentication: internal attack detection	49
3.4	The Importance of A Secure Location Service	53
3.5	Summary	54
4	Location Update Protection for Geographic Routing	57
4.1	A Secure Location Service	58
4.1.1	Assumptions	58
4.1.2	Neighbor Verification for Geographic Forwarding	59
4.1.3	Securing Location Service	61
4.2	Security Analysis	65
4.3	Performance Evaluation & Simulation Results	68
4.3.1	Simulation Scenario	68
4.3.2	Results and Discussion	70
4.4	Extended Discussions	77
4.4.1	Location Update: The Key Protection	77
4.4.2	Alternatives of Local Location Update Protection	78
4.5	Summary	87

5	Location Privacy Preservation in Geographic Routing	89
5.1	Introduction	90
5.2	Anonymized Geographic Ad Hoc Routing	92
5.2.1	Threats Analysis	92
5.2.2	Anonymous neighbor table (ANT)	94
5.2.3	Anonymous greedy forwarding(AGFW)	97
5.2.4	Anonymous location service (ALS)	101
5.2.5	Security Analysis	103
5.2.6	Performance Evaluation	104
5.3	Location Mixing for Preserving Location Privacy	108
5.3.1	Introduction	108
5.3.2	Resolution-Reduced Geographic Routing (RRGR)	109
5.3.3	Implementation & Simulation Results	111
5.3.4	Analysis & Discussion	114
5.4	Summary	119
6	Conclusion	121
6.1	Summary of Research	121
6.2	Future Work	123
	References	129

Abstract

A mobile ad hoc network consists of a collection of wireless mobile nodes that cooperate to forward packets via multiple hops without any fixed infrastructure. MANETs are superior in fast deployment and often designed for some special environments lacking of enough existing network infrastructures. However, MANET is particularly vulnerable to malicious attacks due to its underlying characteristics, such as, wireless open medium, dynamic topology, distributed cooperation, lack of physical protection, etc. Routing design is one of the most important research areas both for security and other network topics. Unfortunately the published work on routing security is relatively limited, and most of the prior efforts are based on some prominent on-demand routing protocols. Our work focuses on the location-based routing or alternatively geographic routing. As another important class of ad hoc routing protocols, it particularly lacks in-depth study of security issues, which has been already considered a major barrier for any kind of ad hoc networks to be put into practice.

In this thesis, we present our work through our intensive research on the topic of securing geographic routing for ad hoc networks. Besides being an important study of security issues of geographic routing, our work makes contribution in two aspects of network security, i.e. traditional security and privacy. To achieve traditional security goals, we proposed a few authentication mechanisms to protect geographic routing from varieties of malicious attacks. By making use of network redundancy, we also proposed a secure location service that takes care of byzantine behaviors as well as benign network failures. Simulation results show that our schemes achieve security goals with quite controlled overheads. For the other side of security, we proposed some protocols taking care of the concern of location privacy which is drawing more and more attentions nowadays. One of the basic ideas in our proposals is to dissociate user identity and location

information so as to anonymize geographic routing where location has to be present. The other approach we considered is to reduce the location resolution used in geographic routing. With a quite different nature of protection, this approach does not apply any cryptographic techniques. Our analysis and simulations show its possibility of protecting location privacy as an alternative, and the routing performance and the level of privacy are well balanced through a controlled location resolution reduction.

List of Publications

- Journal papers:
 - ▷ Z. Zhou and K. C. Yow, “Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy”, *International Journal of Network Security*, Vol. 2, No. 3, pp. 210-218, 2006. (extended version of the work published in MDC’05)
 - ▷ Z. Zhou and K. C. Yow, “Geographic Ad Hoc Routing Security: Attacks and Countermeasures”, *Ad Hoc & Sensor Wireless Networks*, Volume 1, Number 3, pp. 235-253, 2005.
- Conference papers:
 - ▷ Z. Zhou and K. C. Yow, “Location Update Protection for Geographic Ad Hoc Routing”, In *Proceedings of the 10th IFIP Conference on Personal Wireless Communications (PWC’05)*, Colmar, France, August, 2005.
 - ▷ Z. Zhou and K. C. Yow, “Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy”, *3rd International Workshop on Mobile Distributed Computing (MDC’05) In conjunction with the 25th Int’l Conf. on Distributed Computing Systems (ICDCS’05)*, Columbus, Ohio, USA, June 5-10, 2005.
 - ▷ Z. Zhou, K. C. Yow, and S. Nandi, “A Secure Location Service in Mobile Ad Hoc Networks”, In *Proceedings of the Fifth IEEE International Conference on Mobile and Wireless Communications Networks(MWCN 2003)*, Singapore, September, 2003.

List of Figures

2.1	Worm hole attack	15
2.2	Black hole attack(Illustration courtesy of [1])	16
2.3	Routing loop(Illustration courtesy of [1])	18
2.4	Watchdog	24
2.5	Verifier collision	25
2.6	Receiver collision	25
3.1	Greedy forwarding strategy.	35
3.2	Topology dead end. Recovery is required.	36
3.3	Misdirection.	40
3.4	Perimeter forwarding in GPSR.	41
3.5	Black hole attack.	42
3.6	Routing loop.	43
3.7	Selfish node.	44
3.8	Sybil attack and Wall blocking.	45
3.9	Misbehavior detection in geographic forwarding.	53
4.1	Location Update: A is updating its location server L_1 in grid P	62
4.2	Location Query: B initiates a query to A 's location server L_1 for A 's location.	63
4.3	MVLQ: B queries m location servers from S_1 to S_m	68
4.4	Query success ratio as a function of the number of nodes. Nodes move at speeds up to 10 m/s.	70
4.5	Average query delay as a function of the number of nodes. Nodes move at speeds up to 10 m/s.	71

4.6 Query success ratio as a function of the node mobility in the network of 50 nodes. 72

4.7 Normalized packet overhead as a function of the node mobility in the network of 50 nodes. 73

4.8 Normalized byte overhead as a function of the node mobility in the network of 50 nodes. 73

4.9 Query success ratio as a function of the number of misbehaving nodes in the network of 50 nodes. Nodes move at speeds up to 10 m/s. 74

4.10 Reliability of location as a function of the number of compromised nodes in the network of 50 nodes in total. 75

4.11 Average end-to-end query delay for the number of replies with identical location which are genuine. 77

5.1 Performance evaluation of the Anonymous Greedy Forwarding (AGFW). 106

5.2 Resolution-reduced greedy forwarding. 110

5.3 Performance vs location resolution 113

5.4 Packet dropping causes 114

5.5 Network diameter and node density effects (Greedy-only) 114

5.6 Forwarding area of a node. 115

5.7 Delivery ratio changes with node density. 117

5.8 RRGR delivery ratio changes with the grid size and node density. 118

List of Tables

2.1	ARAN Route Discovery Example : S - A - B - C - D	22
4.1	m server grids and n' different location in received replies	64
4.2	Simulation Parameters	70
4.3	Local Location Update Scheme 1	81
4.4	Summary of Proposed Schemes	86

Chapter 1

Introduction

1.1 Background

Small and lightweight devices are always the tendency of hardware development due to its evident advantages. Huge, unwieldy and settled computers in an early time become portable laptop computers and Personal Digital Assistants (PDAs). Big fixed phones become mini and portable cellphones. The huge influx of these portable devices into the daily life has greatly extended the range of places where people are able to perform computing. Since network connectivity is becoming an indispensable part of computing environments, the variety of wireless networks have been gaining more and more popularity. Bluetooth [2] wireless technology connects the devices such as mobile phones and headsets in a short-range of communications, typically in a personal area network while IEEE 802.11 [3] provides higher speed and wider area of wireless access to LAN. The added convenience of wireless access, however, brings about many security problems. Since data are transmitted over the open air, communications are vulnerable to attacks ranging from passive eavesdropping to active interfering. Though such attacks are also possible in conventional networks with some tools, they tend to happen more easily due

CHAPTER 1. INTRODUCTION

to the wireless nature. Security problems in Bluetooth and IEEE 802.11 have been widely studied in [4, 5, 6, 7].

As a new wireless networking paradigm, mobile ad hoc networks (MANET) have been proposed to be set up whenever it is needed and when the network infrastructure is not available. A MANET is considered to be a collection of mobile nodes that have the symmetric capabilities and responsibilities, and cooperate to forward packets without any fixed infrastructure, such as access points or base stations. Each node participates in an ad hoc routing protocol that allows it to discover multihop paths through the network to any other node. The design of such an ad hoc routing protocol represents one of the most important research in MANET.

However, recent research [8] indicates that MANETs pose a larger security problem than conventional wired and wireless networks. The underlying features of MANET set great challenges in achieving security. Among different layers, security in the routing layer attracts most research since routing plays an important role in MANETs and it is proved that trivially applying traditional secure routing mechanism into MANETs is infeasible. Current ad hoc routing protocols can be roughly classified into two categories: *topology-based* and *location-based*. Some prominent topology-based routing protocols such as DSR [9] and AODV [10] have been already carefully studied, though the published work in the security issues in this area is still quite limited. Due to the fact that security problem is envisioned to be a major barrier in the practicality of MANET, we are motivated to work in this area, and particularly securing location-based routing will be the major focus of our research, not only because there is a significant lack of work to be done in the area, but the importance of our work increases with that of the application of geographic routing as well. By introducing location information into routing, geographic routing protocols present promising scalability compared with topology-based routing protocols, and receive increasing attentions with the rapid development of positioning

CHAPTER 1. INTRODUCTION

techniques. The prerequisite of geographic routing is that each node is able to determine its physical position. The recent advances in GPS technology enable a lot of lightweight wireless devices to have positioning capabilities through small, inexpensive, and low power consumption GPS receivers. For example, the Motorola i58 and i88 cellphones have GPS capability built-in. The Garmin iQue 3600 is a GPS enabled PDA.

1.2 Mobile Ad Hoc Network Security

A Mobile Ad Hoc Network(MANET) is a network architecture that can be rapidly deployed without relying on pre-existing network infrastructures. Nodes equipped with wireless devices can be highly mobile, leading to a dynamic network topology. However, the limited range of transmission over the radio channel enforces the communication between two far apart nodes to go through multiple hops of transmission. Thus, a node in a MANET acts both as a host and a router to assist in transmitting data to other nodes in its range. This property of MANETs leads to active research in ad hoc routing protocols. [9, 10, 11, 12] are some prominent examples.

1.2.1 MANET Applications

MANETs' fast deployment capability in arbitrary communication environments enables a number of valuable applications:

- **Military Tactical Networks:** The first application of ad hoc networking was in the military domain. Ad hoc networking enables battlefield units to communicate anywhere and anytime, in extremely hostile and bad environment without any pre-existing infrastructures.
- **Personal Area Networks:** The concept of personal area networks is about interconnecting different devices used by a single person, e.g. a PDA, cellular phone,

CHAPTER 1. INTRODUCTION

laptop etc. In this case the PDA or the laptop will connect with the cellular phone in an ad hoc fashion. The cellular phone can then be used to access the Internet. Another example could be when a person holding a PDA comes within the communication range of a printer. If both the PDA and the printer were ad hoc network enabled, the PDA could automatically get access to the printing services.

- **Sensor Networks:** Sensor networks are ad hoc networks consisting of communication enabled sensor nodes. Each such node contains one or more sensors, e.g. movement, chemical or heat sensors. When a sensor is activated, it relays the obtained information through the ad hoc network to some central processing node where further analysis and actions can be performed. Such sensor networks may consist of hundreds or thousands of sensors and can be used in both military and non-military applications, e.g. surveillance, environmental monitoring etc.
- **Collaborative Networking:** This application of ad hoc networking may be the most intuitive. The simplest example is when a group of people are attending a meeting and need to share information between their laptops or PDAs. If these devices were ad hoc network enabled, they could dynamically set up a network consisting of the meeting participants and thus enable the sharing of the information. Without ad hoc networking, a great deal of configuration and setup would be required to accomplish this task.
- **Disaster Area Networks** Ad hoc networking allows for the quick deployment of a communication network in areas where no fixed infrastructure is available or where the fixed infrastructure has been destroyed by natural disasters or other events. Thus such networks could be used to improve the communication among rescue workers and other personnel and thereby support the relief efforts.

1.2.2 Security Concerns

The characteristics of MANETs raise important security concerns:

- **Ease of Sniffing:** the shared nature of the wireless medium allows anyone in the range of the sender to hear the ongoing transmission, which strengthens and facilitates passive attacks like eavesdropping. The attacker does not even need to approach the wired link nor employ dedicated devices to capture the signal as done in conventional wired networks.
- **Limited Resources for Security:** Many wireless devices have limited CPU capability and storage to meet different restrictions such as cost and engineering difficulty. Besides the little computing resources, limited network bandwidth is another problem that restricts the design of security protocols and applications.
- **Physical Vulnerability:** Usually, nodes in conventional networks are under much better physical protection since critical nodes like routers and servers can be locked in some secret and secure places which only authorized administrators know and are capable of accessing. For mobile hosts, their movement or location is usually not limited, and hence they can be easily captured or hijacked while roaming in a hostile environment. Furthermore, wireless devices are usually small and hand-held ones and can easily be lost or stolen, or possibly tampered with for fraudulent use.
- **Cooperation Requirement:** All wireless devices have a limited communication range. Communication with the node beyond the communication range requires that some nodes between the two parties forward packets. In conventional networks, there are some dedicated nodes called routers for forwarding packets. In MANETs, every node becomes a router. Thus, successful and secure communication heavily depends on the cooperation of users themselves. Accordingly, extra efforts have to be made to enforce node cooperation or to protect against non-cooperation.

CHAPTER 1. INTRODUCTION

- **Service Availability:** Mobile devices usually operate on limited battery power. They may be frequently powered off to save energy or finally drained out, leading to the potential disconnection of the network. Another cause of the irregular connectivity is the dynamic topology. Due to the node movement, the network topology keeps on changing. As a result, some nodes may not be reachable all the time. This irregular nature of network connectivity raises the concern of availability to security services.

The broadcast nature of wireless medium and the weak physical security aggravate the threats to security in MANETs as compared to conventional networks. On the other hand, the decentralized nature of MANETs, potentially poor availability and the strong cooperation requirement set great challenges to achieve security. Any centralized services in a MANET environment cannot be relied upon since they may be out of reach or be powered off, and may be subjected to a single point of failure caused by denial of service(DoS), etc. The performance of basic protocols heavily depend on the cooperation of nodes. Any violation of the basic mechanisms from malicious nodes can cause system failure or severe performance degradation. For example, in contention-based MAC protocol, nodes compete for transmission over the channel. Malicious node may flood the network with packets, take over the channel and cause DoS. In the network layer, misbehaving nodes might also arbitrarily drop packets, though they had agreed to cooperate in advance.

1.2.3 Security Requirements

Clearly, it is not possible for a single security mechanism to fit all situations and requirements. Security requirements depend very much on the kind of mission that has been conceived, and the environment in which it has to operate. Conventionally, the following security requirements or services are considered to secure any data communication, including an ad hoc network:

CHAPTER 1. INTRODUCTION

Confidentiality ensures that the information transmitted is never disclosed to unauthorized entities. Usually, cryptographic encryption is the main approach to achieve this goal. Confidentiality is actually the protection against passive attacks.

The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

Authentication enables a node to ensure the node with which it is communicating is the one it claims to be. Without authentication, a malicious node could disguise as another node to gain unauthorized access to some resources or sensitive information with the consequences left on the victim node. Authentication addresses the protection against active attacks like masquerading.

Data Integrity guarantees the message received is never maliciously modified, or corrupted due to the benign transmission failures such as the burst channel errors. Common checksum algorithms, such as CRC-32, are often used to guard against transmission errors but pose no challenge to malicious adversaries [5]. Cryptographic checksums, such as Message Authentication Code(MAC)(e.g. HMAC [13]), provide much stronger integrity protection.

Non-repudiation ensures that the origin of a message cannot deny having sent the message. It is especially valuable in business or commercial scenarios to arbitrate conflicts. In addition, it is an important evidence for charging misbehaving nodes by revealing that the false information is exactly provided by that node.

Availability requires the network service or resource to be available at anytime. The denial of service attack(DoS) is the main threat to availability in addition to some

CHAPTER 1. INTRODUCTION

network properties like transient connectivity and limited energy. The DoS attack can be launched at several layers of an ad hoc network such as jamming or interfering in the physical layer, disrupting routing in the network layer, and blocking the service by using TCP SYN flooding [14] in higher layers.

Generally, confidentiality, authentication, and strong integrity all require cryptographic keys, which raise the issue of key management. It is another important topic of security which will not be addressed in this thesis.

1.3 Contributions of the Work

Security research for ad hoc networks has been quite limited, though it is undoubtedly considered one of the most important issues to be cleared for the deployment of this new networking paradigm. Based on our careful study of the literature, we identified one of the most lacking area in security research for ad hoc networks, i.e. geographic routing security. The importance of this class of routing in practical applications such as sensor networks brings about our major motivation of this work.

A comprehensive study of geographic routing security We had carefully identified the attacks and threats in geographic routing, and accordingly considered some potential solutions to handle those problems. A link level authentication is considered effective to isolate external attackers, but incapable of handling internal attackers. We also provided a preliminary discussion of some potential techniques to detect malicious modification, forwarding misbehavior and anomalous traffic leading to denial of service.

A secure location service The security in location service is very important for the whole system in geographic routing. Since there is no dominating location service scheme available, the solution to protect location service may depend on the specific

CHAPTER 1. INTRODUCTION

scheme used. Flooding-based location service is suitable for small networks while proxy-based location service is more scalable. We proposed a secure location service based on DLM [15], which isolates unauthorized nodes and provides authenticated location update and query with potentially reliable packet forwarding. Considering the existence of system failures and compromised nodes, we also proposed Majority Voting for Location Query [16] to enhance the availability and reliability of obtaining a correct location.

Local location update protection Although a secure location service seems a very essential part of a secure location-based routing protocol, we found that “location update” is the key issue for the functioning of geographic routing. Thus, location update protection for both local and remote nodes become the key of security. We proposed a few schemes [17] for local location update protection, though none of the schemes is perfect, but with pros and cons. These schemes can also be considered for extending to the remote version of location update.

Anonymized geographic routing protocol We address a very critical issue in geographic routing protocols, which is how to guarantee location privacy while location information is used to maintain the efficiency of geographic routing. We circumvent traditional methods like spatial and temporal cloaking [18] to design an anonymous geographic routing for preserving location privacy. Based on the idea of dissociating the identity and location information, we proposed three building components [19] to achieve anonymity of communication as well as to maintain the functionality of a typical geographic routing protocol.

Resolution-reduced geographic routing protocol We further explore an intuitive way of preserving location privacy by reducing the location resolution exposed. Our approach of mixing location proves to be able to maintain routing performance well

CHAPTER 1. INTRODUCTION

within an acceptable range. The analysis also shows that the node density can also help to make a choice between resolution and performance.

1.4 Organization of the Thesis

The rest of the thesis is organized into five chapters. Chapter 2 gives a literature review of the state of art for security in MANETs. Our review mainly focuses on the routing layer. We classify and discuss the possible attacks in existing ad hoc routing protocols where no additional security measure is taken. Important security proposals are also reviewed. In Chapter 3, we make an essential study for security issues in our context, i.e. for location-based routing. In order to protect against those attacks, some proposals are presented in Chapter 4. Proper analysis and simulation results are provided to evaluate our proposals. Chapter 5 put forward the issue of location privacy, which we try to propose solutions and to address from two different perspectives. In the conclusion of the thesis in Chapter 6, a summary of our research contributions and an overview of the future work are discussed.

Chapter 2

Related Works

In this chapter, we present and analyze the major issues in the context based on our understanding, and accordingly to give a basic review to our awareness over the major related work in the literature. We start the discussion by presenting the attack model followed by attack taxonomy summarized from our study. From our understanding, the research work in this area is considered to be a multi-disciplined effort in different aspects of security. Most of the current efforts could be classified into three major topics, i.e. secure routing, cooperation issue, and key management. Important research works are reviewed respectively.

2.1 Attacker Model

For conventional classification [20], malicious attacks could be mainly divided into two classes: *passive attack* and *active attack*. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation. In the following, we introduce another useful means of classifying security attacks which is more often referred in the literature to suggest threats to ad hoc networks.

CHAPTER 2. RELATED WORKS

External Attacker is typically an unauthorized node that does not belong to the network and does not share any security context with the network. It usually attempts to break into the network or disrupt the functioning of the protocol by eavesdropping, masquerading, modification, and fabrication.

Internal Attacker is unfortunately an authorized node that is compromised for some reasons. For instance, the wireless device is under the control of an attacker, or an exasperated employee maliciously operates. Such a node is much more dangerous than an external attacker since it belongs to the network and has the access to all cryptographic keys in the device. Security violations are not easily detected by basic security mechanisms since internal attackers could provide valid authentication information to access the network resources. Furthermore, the detection of such an attacker through the observed misbehavior is not so straightforward as expected because some normal characteristics of ad hoc networks, such as packet collisions, burst channel errors, and topology changes raise the similar results that are hard to distinguish.

In addition to classifying attacks by internal and external attacks, some other factors can be considered to have a more specific attacker model for analysis. For example, the number of attackers, the number of attackers that could collude, and the computation and communication resources owned by the attacker. Moreover, it may be useful to consider the mobility capability of the attacker, where some restrictive assumptions on speed of an adversary or the reachability of certain areas in another word can be made.

2.2 Types of Attacks in MANETs

Network security should be considered a multi-layered issue rather than any single level of defense against security violation. We always have a few assumptions before making any security analysis. In this section, we present possible attacks mainly targeting on ad hoc

CHAPTER 2. RELATED WORKS

routing protocols. Attacks in physical layer and MAC layer are beyond the scope of this work. The use of spread spectrum has been studied for protection against jamming [21]. Security issues in MAC are studied in [22].

2.2.1 Elements of Routing Attacks

Routing attacks aim at interfering with the function of the routing protocol: discovering and maintaining routes to all desired destinations. All routing attacks rely on the appropriate use and composition of several basic attack techniques:

Packet interception: A malicious node may eavesdrop on packets not destined for itself and learn various information from them, such as the existence or adjacency of nodes. The broadcast nature of physical medium makes such a passive attack much easier to launch and harder to detect in MANET. Moreover, the promiscuous mode of some off-the-shelf equipment or modifying driver settings provides the attack practicality.

Packet modification: If a packet passes through the malicious node, it can deliberately modify some fields in the packet to launch some attacks. Packet modification is mainly used to fool with the false information those nodes that are expecting the packet.

Packet forgery: is a stronger form of modification. It neither requires being on the path between the sender and the receiver, nor is it necessary for a packet to be sent by the sender. A malicious node may forge routing information in the name of another node as well as itself.

Packet spoofing: is another form of forgery. By masquerading as another node, a malicious node may send packets and launch attacks with the consequence left to the victim node.

CHAPTER 2. RELATED WORKS

Packet dropping: A malicious node may drop packets arbitrarily. Routing packets loss could disrupt normal function of the network and prevent a node from obtaining the important information for routing, which severely degrades the performance of the network.

Packet replay: A malicious node can keep old messages and replay them at a later time. If a node is not capable of forging or decrypting packets, replay attack is frequently used to confuse the routing protocol or achieve goals similar to forged messages. In order to replay messages, they just need to be observed previously.

Path interposition: In a mobile ad hoc network, nodes can move around, and it is sometimes advantageous for a malicious node to interpose (i.e. be on the shortest path) between two nodes targeted for attacks.

Wormhole: Wormhole is a quite subtle attack which is elaborately addressed in [23]. In this attack, more than two attackers can establish a “wormhole” and “tunnel” packets from one point of the network to another. If the tunneled distance is longer than the normal wireless transmission range, it is quite easy for the attacker to make the tunneled packet arrive sooner than other packets transmitted through the normal multi-hop route. The attacker can implement the tunneling by the use of, for instance, a single long-range directional wireless link or through a direct wired link to a colluding attacker.

If the attacker performs this tunneling with honest intentions, no harm is done since it is actually enhancing the connectivity of the network. However, the wormhole can be exploited in a variety of ways to launch attacks. For example, it can be used against an on-demand routing protocol such as DSR [9] or AODV[10]. In Figure 2.1, M1 and M2 are colluding malicious nodes. Each ROUTE REQUEST packet from the source node S is tunneled through the wormhole established by M1 and M2 directly to the destination

Figure 2.1: Worm hole attack

node D. After receiving the ROUTE REPLY, S will believe the route is “S M2 D”, and no other routes than the worm hole will be discovered.

The worm hole attack actually short circuits a normal flow of packets, indicating a false idea of the network topology, which may disrupt the routing protocol.

2.2.2 Sophisticated Attacks

Utilizing these basic techniques, one or more malicious adversaries can implement more intensive attacks on the routing system and host resources. Instances of attacks in prominent on-demand routing protocols are illustrated as follows:

Black hole: The black hole attack is briefly introduced in [24]. By sending forged routing packets, an attacker could route all packets for some destination to itself or some other area in the network where in fact the destination is not located. If the attacker successfully diverts the traffic to itself, it is able to do anything with the packets passing through it, such as dropping packets to perform a denial-of-service(DoS) attack.

Figure 2.2 gives an example of black hole attack in AODV. The attacker M receives the ROUTE REQUEST originated by source S for destination D after it is rebroadcasted by B during route discovery. M redirects the traffic to itself by sending back a forged ROUTE REPLY with a significantly higher destination sequence number for D than

CHAPTER 2. RELATED WORKS

Figure 2.2: Black hole attack(Illustration courtesy of [1])

the one specified in the ROUTE REQUEST. Then, B will specify M as the next hop for destination D. The valid reply coming from D later will be dropped by B since the destination sequence number in it is lower than that in the false reply from M. All subsequent traffic destined for D will be directed toward M. The situation will not be corrected until either a legitimate ROUTE REQUEST or ROUTE REPLY with a destination sequence number for D higher than that in the false reply enters the network. In this case, the attacker M becomes a routing black hole. In addition to modifying the sequence number, the hop count in the ROUTE REPLY can also be modified to attract routes towards the attacker.

Black hole attack in DSR is much more straightforward. An attacker can divert the data traffic by simply modifying the node list in the reply packet or directly forging a reply with a deliberately-constructed node list.

Host resources consumption: An attacker can exhaust resources of a node in some routing protocols. Targeted resources could be CPU, memory or battery.

- Sleep deprivation: The sleep deprivation torture is briefly introduced in [25]. Usually, this attack is practical only in ad hoc networks, where battery life is really a critical factor. Battery powered devices switch to sleep or power saving mode to conserve energy when no network operation or computation is required. An

CHAPTER 2. RELATED WORKS

attacker may attempt to consume battery power by requesting unnecessary routes, or by sending excessive packets to some nodes.

- **Routing table overflow:** In a routing table overflow attack the attacker attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. Proactive routing algorithms attempt to discover routing information even before it is needed while a reactive algorithm creates a route only when it is needed. This property appears to make proactive algorithms more vulnerable to table overflow attacks. An attacker can simply send excessive route advertisements to the routers in a network. Reactive protocols, on the other hand, do not collect routing data in advance. In an attack on reactive protocols, for example in AODV, two or more malicious nodes may cooperate to create false data efficiently: one node requests routes and the other one replies with forged addresses, and false routes can be continuously be advertised so that they push all legitimate routes out of the routing table.

Network resources consumption: An attacker disrupts the whole network by disabling or overloading it to dramatically degrade the performance so that other nodes cannot use the network normally. It may inject extra data packets into the network, which will consume bandwidth resources, especially over routing detours or loops. Similarly, excessive control packets can be injected into the network, causing even more consumption of bandwidth and computational resources since nodes need to do more processing to control packets.

- **Routing loop:** In some protocols routing loops can be created and packets follow the loop until their lifetime expires. Here is an example in AODV. Figure 2.3(a)

CHAPTER 2. RELATED WORKS

shows the original routes towards the destination X in each node. The attacker M can learn this topology by listening to the ROUTE REQUEST/ROUTE REPLY exchanges during route discovery. To start the attack, the attacker M moves close to D and out of the range of A. It then sends a ROUTE REPLY to D with a hop count to X less than the one sent by C. D therefore changes its next hop towards X to A as illustrated in Figure 2.3(b).

M then moves close to C and out of the range of D, and then sends to C a ROUTE REPLY with a hop count less than what E has sent. C then changes to route via D as illustrated in Figure 2.3(c). Thus, later packets for X will follow the loop "A B C D A".

- Detour: If it is situated on the optimal path between a sender and receiver, a malicious node can force the use of another route by dropping route discovery packets.
- Flooding: An attacker may introduce excessive flooding to severely overload the network. As an example, the attacker can inject extra ROUTE REQUEST packets in DSR or AODV which flood throughout the network.

These routing attacks are some of the reasons why simply using traditional end-to-end security mechanisms such as IPSec[26], Authentication Header(AH)[27] or Encapsulating Security Payload(ESP)[28] does not protect ad hoc networks from capable adversaries from disrupting the routing protocol.

2.3 Security Schemes for Ad Hoc Routing

The increased attention to security in ad hoc networks attracts more and more research on this area, though published work in this area is still quite limited so far. In this

CHAPTER 2. RELATED WORKS

Figure 2.3: Routing loop(Illustration courtesy of [1])

CHAPTER 2. RELATED WORKS

section, we review some of the representative secure routing schemes proposed to protect against specific attacks identified.

2.3.1 Ariadne

Hu et al. [29] aim to address routing security and introduce a new routing protocol, Ariadne, based on unoptimized DSR.

Ariadne provides the end-to-end authentication of a routing message using a message authentication code (MAC) and a shared key between the two parties, that is, the target node can authenticate the authenticity of the initiator of the route discovery and the integrity of the message, and the initiator can authenticate that RREP really comes from the expected target and is not modified. Furthermore, Ariadne guarantees that the initiator can authenticate each intermediate node on the path included in the reply by using TESLA [30]. TESLA is the preferred authentication mechanism in Ariadne since it is based on symmetric cryptography and adds only a single MAC to a message for broadcast authentication.

Ariadne introduces a *per-hop hashing* method to prevent the malicious node from removing nodes from the node list in the RREQ. Each intermediate node calculates a new hash chain value with its identity and the old value, and replace it with the new one. In order to change or remove a node from the node list, the attacker must invert the one-way hash function to avoid being detected.

In order to enable the initiator to authenticate all the intermediate nodes on the path, during the route discovery each intermediate node uses the TESLA key for the time interval specified in the RREQ to compute the MAC and appends it to the RREQ. When the target receives the RREQ, it checks its validity and then buffers the RREP until intermediate nodes can release the corresponding TESLA keys. During the propagation of RREP, each node on the path appends its key to the RREP. After receiving the RREP, the initiator can authenticate all the intermediate nodes on the discovered path.

CHAPTER 2. RELATED WORKS

Route maintenance in Ariadne is based on DSR. A forwarding node returns an RERR to the original sender of the packet if it is unable to deliver the packet to the next hop after a limited number of retransmission attempts. Ariadne suggests using TESLA for authenticating the RERRs so that forwarding nodes can also authenticate and process the RERRs.

Ariadne copes with attacks performed by malicious nodes that modify and fabricate routing information, and with attacks by impersonation. However, routing misbehavior from the internal attackers such as compromised nodes is still not addressed in detail nor satisfyingly solved, though the most frequently used method is to make use of redundant routes to mitigate the effects of routing misbehavior.

RREQ flooding attack is also addressed in Ariadne. The attacker can launch a denial of service attack by simply injecting excessive RREQ which floods throughout the network. To protect this attack, Ariadne uses so-called Route Discovery Chains, a mechanism for authenticating route discoveries, which allows each node to limit the rate of discoveries initiated by any node.

2.3.2 ARAN

Sanzgiri et al. [1] identify three different environments with distinct security requirements: open environment, managed open environment, and managed hostile environment, among which they propose a solution, called ARAN, to the managed open environment. ARAN has a route discovery process similar to AODV [10] and is based on the public-key certificate and digital signature scheme.

ARAN mainly provides end-to-end and hop-by-hop authentication. Before sending a route request, the initiator first attach to the route request its certificate and the signature computed over the whole packet for the sake of the authentication of the destination. During the propagation of the route request, each intermediate node first validates the

CHAPTER 2. RELATED WORKS

signature with the given certificate in the received route request, removes the previous signature and the corresponding certificate, and then appends its own signature generated over the whole message. The target, upon receiving the route request, validates the previous hop and the signature of the initiator, and then unicasts the route reply with its own signature back to the initiator. Authentication of the route reply is similarly done based on the hop-by-hop authentication. If a node fails to forward a packet, a route error message is sent back to the original sender of the packet. The route error message does not invoke the hop-by-hop authentication; only end-to-end authentication is applied to avoid malicious nodes from injecting false error information.

An advantage of the hop-by-hop authentication is that the broadcast route request packet flooding attack in Ariadne [29] is not possible since every route request injected into the network should carry a valid signature that will be authenticated at each hop. The external attacker cannot forge a valid signature to avoid being detected.

In order to use public-key certificate scheme, ARAN requires a trusted certificate server, whose public key is known to all nodes, to issue signed certificates to nodes who are going to enter the network. Revocation of the certificate is another critical problem, which is not yet properly solved in the present-day interest. ARAN proposes a way of certificate revocation. The trusted certificate server is responsible to send out a revocation message signed by itself. Each node receiving the message rebroadcasts it to its neighbors. But this method is not fail-safe. The compromised node or the owner of the revoked certificate may not propagate the revocation message to other nodes. That node may still be viewed as a trusted party by part of nodes until the natural expiration of its certificate.

ARAN prevents most of the external attacks through the strong authentication mechanism, and the replay attacks are prevented by including a nonce and timestamp in the routing message. But the possible effects of compromised nodes are not considered nor

CHAPTER 2. RELATED WORKS

Table 2.1: ARAN Route Discovery Example : S - A - B - C - D

$S \rightarrow * :$	$\langle REQUEST, ip(D), cert(S), N(S), t \rangle sig(S)$
$A \rightarrow * :$	$\langle \langle REQUEST, ip(D), cert(S), N(S), t \rangle sig(S) \rangle sig(A), cert(A)$
$B \rightarrow * :$	$\langle \langle REQUEST, ip(D), cert(S), N(S), t \rangle sig(S) \rangle sig(B), cert(B)$
$C \rightarrow * :$	$\langle \langle REQUEST, ip(D), cert(S), N(S), t \rangle sig(S) \rangle sig(C), cert(C)$
$D \rightarrow C :$	$\langle REPLY, ip(S), cert(D), N(S), t \rangle sig(D)$
$C \rightarrow B :$	$\langle \langle REPLY, ip(S), cert(D), N(S), t \rangle sig(D) \rangle sig(C), cert(C)$
$B \rightarrow A :$	$\langle \langle REPLY, ip(S), cert(D), N(S), t \rangle sig(D) \rangle sig(B), cert(B)$
$A \rightarrow S :$	$\langle \langle REPLY, ip(S), cert(D), N(S), t \rangle sig(D) \rangle sig(A), cert(A)$

addressed. Furthermore, piggybacking certificates in routing messages introduces a big packet overhead and consumes much energy to transmit.

2.3.3 Others

SRP [31] mainly introduces authentication to a source route discovery protocol. SRP assumes the existence of shared secrets between all pairs of communicating nodes and uses Message Authentication Code (MAC) to provide authentication of the route request and reply, such that fake requests are not accepted at the destination, and routes in replies cannot be modified without detection. However, route requests cannot be authenticated by intermediate nodes so fake route requests can flood the network. The route as recorded in the packet can also be modified by adversaries without being detected since the route in the request is dynamic during propagation, and is not included in the MAC calculation. SRP deals with this problem by replying to a set of route requests at the destination to provide route diversity, which reduces the possibility of choosing the lengthened routes at the source where the route length is the criterion. One obvious problem is that SRP cannot stop the attacker that is located on the “shortest path” between two communicating parties.

CHAPTER 2. RELATED WORKS

SAODV [32] has been proposed as an extension of the Ad Hoc On-demand Distance Vector (AODV) protocol to protect the routing protocol messages. SAODV assumes that each node has certified public keys of all network nodes, so that intermediate nodes can validate all in-transit routing packets. The basic idea is that the originator of a control message appends an RSA signature [33] and the last element of a hash chain [34], i.e. the result of n consecutive hash calculations on a random number seed. Digital signature guarantees the authenticity of the source and the integrity of the fixed fields in the packet. The use of hash chain value guarantees that the adversary cannot arbitrarily reduce the hop count. As the message traverses the network, intermediate nodes verify its signature and the chain value and generate a new chain value by hashing the old one in the packet. The route replies are provided either by the destination or intermediate nodes having an active route to the sought destination, with the latter mode of operation enabled by a different type of control packets. In fact, the effectiveness of the applied hash chain is based on the assumption that the adversary cannot obtain the previous hop chain value or the original seed when it is m hops away from the source. However, it may not be true if the colluding attackers are considered, for example, the wormhole attack.

SAR [35] introduces the Quality of Protection (QoP) into the route discovery process, sharing the similarity with Quality of Service (QoS) for ad hoc routing. By associating protocol messages with certain quantifiable security metrics, SAR tries to discover the route with the satisfied level of security. In particular, nodes in a MANET subnet are classified into different trust and privilege levels. A node initiating a route discovery sets the sought security level for the route, i.e. the required minimal trust level for nodes participating in the query/reply propagation. Nodes at each trust level share the corresponding symmetric keys. Intermediate nodes of different levels cannot decrypt in-transit

routing packets, or determine whether the required QoS parameter can be satisfied, and will simply drop the packets. Although this scheme provides some protection (e.g. integrity) of the routing protocol traffic, it does not eliminate false routing information injected by malicious nodes. Moreover, the proposed use of symmetric cryptography allows any node to corrupt the routing protocol operation within a level of trust by mounting any attacks that are possible without the presence of the scheme. Finally, the assumed supervising organization and the fixed assignment of trust levels may not be practical for MANET.

2.4 Cooperation for Ad Hoc Networks

Till now, no mechanisms have taken the misbehavior from the compromised or byzantine nodes into consideration. Even though a trusted route can be established by applying some security mechanisms into the route discovery, potential node misbehavior may also exist during packet forwarding because of the existence of compromised nodes.

2.4.1 Watchdog and Pathrater

Marti et al. [36] proposed two extensions to DSR [9], watchdog and pathrater, to detect and mitigate routing misbehavior. The watchdog identifies misbehaving nodes, while the pathrater avoids routing packets through these nodes.

Watchdog assumes a symmetric link between two nodes, which means that node A will be in node B's transmission range if B is in A's transmission range. Figure 2.4 illustrates how the watchdog works. Suppose there exists a path from node S to D through intermediate nodes A, B and C. If A forwards a packet to B who is supposed to forward to C at the next hop, A can listen to B's transmission to check whether B has correctly forwarded the packet.

CHAPTER 2. RELATED WORKS

Figure 2.4: Watchdog

Clearly, for the watchdog to work properly, it must know the next two hops of a packet at least. So, watchdog only works best on top of a source routing protocol such as DSR. Watchdog is also not power efficient since each node needs to be at receiving state, even though it has no data to transmit. In addition to these limitations, watchdog has some other weaknesses:

Verifier collision: As Figure 2.5 illustrates, a packet collision may happen at verifier A to prevent it from overhearing the transmission of B, which is indistinguishable from the misbehavior that B did not forward the packet. Because of this uncertainty, there is a threshold rate specified in the watchdog.

Receiver collision: A packet collision may also happen at the receiver C as illustrated in Figure 2.6, which causes A to believe that a packet has been transmitted when it hasn't in fact. If B is malicious, it can even purposefully cause the collision by pausing to forward until C is transmitting.

Partial dropping: Due to natural sources of errors such as collision, watchdog has a dropping rate threshold. A malicious node can stay right under this threshold and

CHAPTER 2. RELATED WORKS

Figure 2.5: Verifier collision

Figure 2.6: Receiver collision

avoid detection. Although such misbehavior is not detected, the watchdog enforces a minimum bandwidth.

Slander: Watchdog is quite vulnerable when a node falsely accuses other nodes of misbehaving. A malicious node could attempt to isolate some nodes by claiming that they are misbehaving. For instance in Figure 2.4, A could report that B is not forwarding packets when in fact it is. This will cause S to mark B as misbehaving and to void routing packets through B. However, this behavior may be detected since receiving acknowledgments from D indicates that B is working properly. If A drops acknowledgments to hide the fact, then B will detect this misbehavior and report it to D.

Controlled transmission power: Another problem is that controlling transmission power well can circumvent the watchdog. A misbehaving node could limit its transmission power such that the signal is strong enough to be overheard by the previous node but too weak to be received by the true recipient. However, having the capability of power control is required for nodes to behave in this manner.

Colluded misbehavior: Two consecutive misbehaving nodes could collude to circumvent the watchdog. For example in Figure 2.4, B forwards a packet to C but does not

CHAPTER 2. RELATED WORKS

report to A when C drops it. This is a kind of more sophisticated and powerful attack which is not easy to solve.

Pathrater, the second scheme, maintains a per node reliability rating. The reliability of every path to a destination is assessed by averaging each node's rating along the path, and the highest is chosen to send packets. When pathrater learns about a new node, it assigns a default value of 0.5. The ratings of nodes along the active path are incremented by 0.01 at periodic intervals of 200 ms. The active path is one in which a packet has been sent within an interval. The maximum value a node can achieve is 0.8. If a link/routing failure is detected, the rating of the node on the path which cannot be reached is decremented by 0.05 down to a minimum of 0. Malicious nodes identified by watchdog are assigned a reliability score of -100. A reset timer on malicious nodes is suggested, but has not been studied.

2.4.2 Other approaches

The previous approach is detection based. Another approach called cooperation enforcement is charging and rewarding based, which usually attempts to provide incentive to nodes for their compliance with the protocol rules, i.e. properly relay user data. L. Buttyan and J. P. Hubaux [37] introduced a concept of fictitious currency, which enhances the service availability. A third approach to mitigate misbehavior is reputation based. It attempts to build a reputation system [38, 39] which regulates node behaviors.

2.5 Security Association Establishment

In this section, we review the key setup solution behind those important secure routing protocols. Security protocols typically depend on cryptographic techniques that require prior setup of security associations among nodes before the protocol is applied, specifically key setup or distribution. The process of establishing security associations itself

CHAPTER 2. RELATED WORKS

needs to bear security in mind, which radically implies the underlying “trust model or establishment” assumed in the application.

Ariadne Ariadne [29] discussed the approach of Key Distribution Center(KDC) to support its authentication for DSR. A Key Distribution Center(KDC) has a shared master key with each node, or every node has its authentic public key, or every node has its authentic TESLA commitment key. Thus, KDC initiates a special route discovery to find routes to all nodes, and individually transmits encrypted and authenticated keys to them. They are able to authenticate and decrypt the keys to use.

Setting up shared keys requires authenticity and confidentiality whereas setting up public keys only requires authenticity. For setting up pairwise keys, the KDC needs to find a route and sends the encrypted key to every node individually. The pairwise keys are encrypted with the destination’s public key or shared master key. For setting up of public keys, it could be an on-demand distribution since nodes can authenticate other’s public key by KDC’s public key, assuming every node’s public key is signed by KDC. Alternatively, public keys are broadcasted by KDC. Two alternatives are nothing but tradeoff between storage and communication/computation overhead.

We consider the following problems for Ariadne:

- Since key setup also relies on the underlying network delivery function, which is, however, the service we are trying to guarantee by carrying out protections. To avoid the circular security dependency, Ariadne proposes to bootstrap nodes by delivering all keys needed. Obviously, it is undesirable in terms of storage requirement for ad hoc nodes, and also from the scalability point of view.
- If it is supposed to be an on-demand delivery of keys to reduce the storage burden, KDC has to be online for shared key agreement since nodes have only its shared master key with KDC or has only authenticated its public key to the trust entity. As

CHAPTER 2. RELATED WORKS

a consequence, potential communication overhead delays are inevitable. For public key distribution, the trusted entity may not need to be online if we do not consider other issues related to the certification scheme, such as certificate revocation.

SPINS: Security Protocols for Sensor Networks SPINS [40] mainly proposes two protocols: SNEP and uTESLA. SNEP offers “semantic security” by using CTR mode of block cipher, so that the input of encryption is never same, which means that even for the same text to encrypt, you will get the different ciphertext. In order to use CTR mode, the counter value needs to be synchronized. Therefore, SNEP provides a simple authenticated exchange protocol. Furthermore, for security concern, SPINS argues to use different keys for encryption and MAC computation. uTESLA is a straightforward application of TESLA in sensor networks. The only difference is that the initial commitment key is authenticated by the shared key, or is directly authenticated through the base station since each node is assumed to have a master key with the base station. Furthermore, the storage of key chains of the sender could be released by storing them on the base station.

So, SPINS’s key setup is fairly simple, i.e. it preloads the shared master key in each node with the base station. Once a node has a shared key with the base station, it can agree on shared keys with other node via the base station.

Distributed CA Using Threshold Cryptography Zhou [41] proposed k servers, k specially designated nodes in the network, for distributing the task of a CA using a secret share algorithm, and prevents mobile adversary by employing a proactive secret share update algorithm. Kong [42] extended the idea of threshold cryptography and proposed a detailed scheme which distributes the CA functionality to all nodes. Every joining node could obtain its share of the system’s private key from any k nodes, e.g. its k neighbors. But the value k could be the trade-off of availability and robustness.

CHAPTER 2. RELATED WORKS

Furthermore, it seems to be vulnerable to the “Sybil attack”, an attack that can take as many identities as necessary to collect enough shares and to reconstruct the system private key. This problem boils down to the question of how a node is admitted into the network, and how it performs exchanges to obtain its certificate. This may very much depend on the specific ad hoc context.

Self-organized PKI Capkun et al. [43] proposed a self-organized public key infrastructure (PKI) scheme for ad hoc networks. The idea of trust establishment is similar to the PGP web of trust [44]. Users issue certificates to each other based on offline trust relations. If a node A wants to authenticate another node B ’s public key, it only needs to find out a chain of certificates to the target public key through which it can verify. The problem of this scheme is that the trust establishing process could be very slow in practice. Furthermore, the resulting trust relationships among users may be much more sparse than those of general social environments.

Sufficient Trust Establishment Ren et al. [45] considered the sparseness problem of self-organized PKI from the minimal direct relation set required for trust connectivity. At the bootstrap phase, there is a secret dealer who loads each node with a short list of $\langle id, public_key \rangle$ bindings. The preloaded short list is designed in such a way that the probability of finding a chain of certificates(i.e. a chain of trust) to another node is high enough.

From the above reviews of different schemes, we find that current solutions for security association establishment can be roughly divided into two ways: centralized and distributed. For distributed models, the trust is based on either a chain of trust or a confident number of trusted nodes. In other words, the node is authenticated by a chain of trust or a set of member nodes. However, the longer the chain is, the less confident of trust one has. For centralized models, trust is based on the third trust party, KDC or

CHAPTER 2. RELATED WORKS

CA. If the node is certified by a third trust party, it is trustworthy. In fact, Capkun et al. [46] also introduces another way to establishing security association through physical contacts by exploiting node mobility effect, or even through a “friend” where there is no such physical contact possible inbetween. Of course, a fourth way may even be a combination or hybrid of the three.

2.6 Summary

In this chapter, we summarized the main security issues in mobile ad hoc networks, classified possible attacks mainly in the routing layer, and reviewed some prominent works on routing security. Till now, potential effective key management is widely assumed by most of the security mechanisms, which is another big issue for security. Current efforts towards the design of secure routing protocols are mainly oriented to on-demand (reactive) routing protocols such as DSR[9] and AODV[10], where a node attempts to discover a route to some destination only when it has a packet to send to that destination. On-demand routing protocols have been demonstrated to perform better with significantly lower overheads than proactive routing protocols in many scenarios since they are able to react quickly to topology changes, yet being able to reduce routing overhead in periods or areas of the network in which changes are less frequent. It is possible to find, however, interesting security solutions for proactive routing protocols which are worthwhile to mention.

The location-based routing protocol differs from the reactive or proactive routing protocol, and shows superiority in scalability. However, security in this class of ad hoc routing has not received enough attention so far. Our work is dedicated to achieving location-based routing security, which we are going to present in the following chapters.

Chapter 3

A Comprehensive Study of Geographic Routing Security

Geographic routing is a different but efficient routing model. The lack of security protection, however, makes the existing geographic routing protocols only possible to work in a benign environment. They are impractical to be applied to real life environments where malicious intentions exist.

We are the first research effort to give a complete threat analysis to geographic routing in this area. We will explain in details how exactly attacks can be mounted in the geographic routing, and show that not only known attacks in other systems are possible in geographic routing, but also the vulnerabilities that are unique and fatal to geographic routing, such as wall blocking and memory consumption attack to location servers. To protect against these potential security breaches, we consider two lines of defense to compensate for each other, i.e. authentication and post-authentication. Post-authentication will be helpful when internal nodes start becoming malicious that authentication mechanism will hardly be able to take care of.

Before discussing the security problem in detail, we will first give a proper overview and analysis of this type of routing protocols.

3.1 Overview of Location-based Routing

Available routing protocols can be roughly classified into two categories: topology-based routing and location-based routing. Topology-based routing uses the information about links and the network topology to perform packet forwarding. A number of routing protocols such as DSR [9], AODV [10], DSDV [47], etc. belong to topology-based routing. Location-based routing eliminates some of the limitations of topology-based routing by using additional information. The forwarding decision at each node is based on the location of the destination included in the packet and the location of its neighbors.

Every node determines its own location by aid of some positioning system such as GPS [48]. Since it is not necessary to maintain the route information, the location-based routing scales well even if the network is highly dynamic, which is the main advantage of it. The prerequisite for this kind of routing is that the sender must have the knowledge of the location of the destination, which is main task of a location service. Mauve et al. [49] conclude that location-based routing typically has two building blocks: *forwarding strategy* and *location service*.

3.1.1 Forwarding Strategies

To deliver a packet from the sender that has the destination's position, intermediate nodes should apply certain strategies to make forwarding decisions so that the packet can be delivered to the destination in an efficient and cooperative manner.

Quite a few greedy forwarding strategies have been proposed in the literature. One of the most intuitive strategies [50] is to forward packets to the neighbor closest to the destination as illustrated in Figure 3.1. S chooses I , the closest neighbor to D . A slightly different strategy is Most Forward within Radius (MFR) [51]. It chooses the one with the largest progress on the straight line between sender and destination. The goal is to minimize the number of hops a packet has to traverse in order to reach

Figure 3.1: Greedy forwarding strategy.

the destination. However, in [52], it is shown that a Nearest with Forward Progress (NFP) strategy performs better than MFR in favor of power saving and the likelihood of successful transmissions. NFP is basically a reverse MFR. Rather than choosing the neighbor with the largest progress, the shortest one is considered. Another strategy for forwarding packets is compass routing, which selects the neighbor nearest to the straight line between sender and destination, i.e. the transmission angle directed to the destination is minimized. The goal of compass routing is to minimize the spatial distance to travel.

Unfortunately, greedy forwarding strategies may fail to find a path to the destination when the network topology has dead-ends, or typically referred as “local maximum”. An example of local maximum for the first greedy strategy we discussed is illustrated in Figure 3.2. X cannot forward the packet because there is no node inside its range that is closer than itself to D .

To avoid a direct abortion, certain recovery procedure is required when local maximum occurs. The face-2 algorithm [53] and the perimeter mode of Greedy Perimeter Stateless Routing Protocol(GPSR) [50] are two similar recovery approaches based on planar graph traversal. A packet enters the recovery mode when it arrives at a dead-end, and it returns to greedy mode when it reaches a node closer to the destination than the node

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

Figure 3.2: Topology dead end. Recovery is required.

where the packet entered the recovery mode. Both recovery approaches do not require the nodes to store additional information. Therefore, with recovery mode, geographic routing schemes retain the ability to make localized forwarding decisions. A more latest work called GOAFR [54] has a better combination of greedy and face routing to achieve worse case optimal as well as average case efficient.

DREAM [55] and LAR [56] are some other examples of geographic routing protocols. In DREAM, the sender forwards packets towards the expected region of the destination. The expected region is usually estimated by the location and the speed of the destination. LAR actually does not define a geographic routing protocol but represents an enhanced on-demand routing protocol by using location information. LAR incorporates a location metric to restrict the route discovery flooding frequently used in on-demand protocols to a certain area, the request zone. A request zone for the route discovery is computed based on the expected zone and the location of the source. Like in DREAM, an expected zone is an estimate of the possible region of the destination, which is computed based on the location and speed of the destination. LAR does not specify any location service. The knowledge of other nodes' location is expected to be learned from the initial routing message exchanging, which can piggyback the location of the communicating parties.

3.1.2 Location Services

Location service is an important service for the sender to learn its target's position. However, the fact that location service should be provided by the ad hoc network itself presents a chicken-and-egg problem [49]: without a location server, it is not possible to get location information; without the location information, the location server cannot be reached. Therefore, a few location service schemes have been proposed to address the problem of how a node obtains the location of the requested node. Basically, we can group them into two categories: flooding-based and proxy-based.

In DREAM, the location service is provided by requiring that each node proactively flood location updates throughout the entire network, which allows all nodes to build a location database of the other nodes. To limit network-wide flooding, DREAM stops location updates from propagating out of a specified physical distance based on the so-called “distance effect”. As the authors argue, “the greater the distance separating two nodes, the slower they appear to be moving with respect to each other.”

GLS [57] and DLM [15] are two examples of proxy-based location services. GLS divides the network area into a hierarchy of grids. Every node distributes its location information to some nodes in a different grid level which are designated as its location servers when they have the “closest” ID to its own ID in that level. A node can query for the location of the expected node by executing the query process to approach the location server of its level for that node. GLS works fairly well in stationary networks. However, it becomes less efficient when node mobility is considered. In order to find a location server in a certain level, a node needs to potentially or indirectly scan the entire region to find out the node with the “closest” ID. Usually, an update or query packet will go several steps to reach the specific location server. When node mobility is considered, such a “closest ID” property appears to be difficult to maintain, that is, frequent location

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

server change causes increasing out-of-date information and accordingly more location query failures.

DLM brings a different idea of identifying a node's location servers. It is also called homezone based location service. Instead of using the concept "closest ID", location servers are selected by hashing the node's ID to several grids, its homezones, that contain its location servers. DLM provides two policies for location update and query: Full length address policy and Partial length address policy. In the full length address policy, location servers are periodically updated at a low rate. In addition, each time when a node moves away from its original grid, it needs to update all its location servers. If a node A wants to query for another node B's location, it simply hashes B's ID to some grids that contain B's location servers, and chooses the closest grid to make its query. After receiving the reply with B's full length address, A can use it to contact B for accurate location information. The problem of the mobility of servers in DLM will not be as significant as in GLS since grids are fixed, although the nodes are moving.

3.2 Attacks on Geographic Routing

In topology-based routing, the goal of attacks is typically to prevent the network from finding a valid route or to permit finding a route only if it includes the attacker by manipulating the route or routing information. In geographic routing, the same goals are achieved by manipulating the location information. In this section, we address most of the identified attacks in geographic routing. We use forwarding strategies in [53, 50] to illustrate all attacks.

Before describing the attacks, we will first analyze how nodes are supposed to be cooperative in the geographic protocol.

3.2.1 Analysis of cooperation

Current geographic routing protocols are designed under an assumed environment where all nodes are trustable. However, in a more realistic setting, nodes are not expectedly cooperative. We analyze the cooperation assumptions as follows:

- R1*: Every node is supposed to indicate its *presence* to neighbors, which enables an effective forwarding scheme based on the fresh neighbor information. A node may agree to cooperate and forward packets because in return it expects to enjoy the network service, such as sending and receiving packets. Without indicating its presence, the node cannot receive the network service.
- R2*: Every node is supposed to update its *genuine* location to neighbors, which enables a correct forwarding based on the genuine information. The only reason for a node to do so is to respect the agreed protocol.
- R3*: Every node is supposed to *obey* the location service protocol, which enables a querying node to obtain a fresh and reliable location of the requested node. For example, in the flooding-based scheme, intermediate nodes are supposed to propagate the location query packet in a protocol manner. In some location proxy-based schemes, nodes are supposed to behave as a location proxy for other nodes, if selected according to the protocol, to store clients' location and to respond to queries. The reason for a node to cooperate in a location service is only to respect the agreed protocol.

R1 indicates that every node is free to decide its updating policy to balance between its privileges and responsibilities for the network. For example, a node which updates its neighbors actively will receive more services but will also be asked to relay more packets. In some location services, a node which stops updating its location servers indicates to refuse future communication requests from remote senders.

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

R2 and *R3* require protocol level cooperation. Malicious nodes may not respect the protocol as expected, leading to different attacks. How easy it is for an attacker to manipulate the physical hardware and software in a node in order to change the behavior of the protocol depends on the specific design of the software system for a node. It is fair to assume that the malicious node is able to change the operations of the protocol somehow in the system level software.

Therefore, we believe that the main security issues in geographic routing will come from the violations of *R2* and *R3*. *R1* is not significant from the security point of view.

3.2.2 Forwarding misbehavior

There are four possible forwarding misbehaviors: suppression, misdirection, modification and replay.

Suppression refers to dropping packets on purpose rather than from network congestion or because there is no route to the destination. There are several possible reasons for this misbehavior. Nodes in MANETs tend to be selfish and reluctant to relay packets for others in order to save their battery life. Some malicious nodes may attempt to block the interested communication by dropping all packets from or to the target node. Instead of suppressing all packets, a more sophisticated attacker may selectively drop packets such that it is enough to make trouble for the target communication but not enough for a detection mechanism to identify the misbehavior. Due to the potential sporadic connectivity in ad hoc networks, it becomes much harder to differentiate the benign network failure and the malicious packet dropping.

Misdirection refers to forwarding packets not in accordance to the protocol. Misdirecting in geographic routing may not cause big harms but it degrades network performance. The misdirected packet in greedy forwarding, for example, still has the chance to reach the destination but experiences a longer end-to-end delay. That is because the packet

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

will still be forwarded towards the destination. For example, in Figure 3.3, although X misdirected the packet to C rather than to B according to greedy forwarding, the packet will still reach D via C , E , and F .

A simple bounce-misdirection could also be possible. For example, in Figure 3.3, the node X just passes the received packet back to the previous hop A . Since A is not aware of this misbehavior, it only knows that it received another packet destined for D , and therefore will forward the packet to X again according to greedy forwarding, causing a bouncing packet between A and X .

It is similar in perimeter forwarding of GPSR that the packet misdirected will also have the chance to reach the destination. If the packet does not fall into a loop, it will keep on being forwarded along the perimeter until it jumps out of the perimeter mode or reached the destination. Figure 3.4 illustrates the possibility of delivery success and failure respectively.

The packet from S will reach the local maximum at X . X then sends it to B in perimeter mode. B is supposed to forward to E according to the right hand rule. But it misdirects the packet to C . Fortunately; the packet will be still able to reach the destination via C , G , E , F , D according to GPSR. However, if B misdirects the packet to A , then the packet falls into a loop according to perimeter forwarding, and hence it will be dropped when it reaches X for the second time.

Figure 3.3: Misdirection.

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

From the above discussion, we know that misdirection is not as frustrating as suppression since the packet could reach the destination with chance. It may, however, degrade the network performance such as increasing longer delays, and wasting more bandwidth.

Modification could happen before forwarding. Usually some end-to-end authentication mechanism such as Message Authentication Code (MAC) is employed to protect the integrity of the packet. These mechanisms only protect the receiver from accepting the corrupted data. It has no way to detect where the packet was modified nor who has done it. So, the malicious node faces no risk in modifying packets and causing trouble to the network communication. For example, if the destination's location is modified, the packet will not be able to reach the expected destination, and the modification misbehavior is difficult to detect. Furthermore, modification makes trouble not only to end parties but also to the network itself. Fake traffic traveling in the wrong way leads to undesirable network overhead or bandwidth wastage, especially in the resource constrained ad hoc networks.

Some detection mechanisms must be available to solve the detection problem as well as be an effective deterrent. However, the position where this type of real time detection can take place is only within the range of the attacker. To mitigate the error in detection,

Figure 3.4: Perimeter forwarding in GPSR.

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

Figure 3.5: Black hole attack.

cooperative detection may be required.

Replay refers to transmitting packets intercepted before. It will not be significant if some higher level techniques are applied such as sequencing or timestamping.

3.2.3 Malicious attacks

Black hole: In this attack, the traffic of the sender will be directed to a place the attacker specified. If the attacker suppressed all packets received, it looks like a black hole in the traffic. In geographic routing, this attack can be easily mounted by sending Hello messages with a false location. For example, in Figure 3.5, the malicious node M sends a hello message to B with location $(1, 4)$ instead of its real location $(2, 3)$. B will forward all packets destined for D to M because it knows M is closer to D than C . This example is based on greedy forwarding, and of course, there are corresponding variations of the attack targeted on other forwarding strategies.

Wormhole: This is a quite subtle attack in MANETs. Two colluding attackers can utilize an out-of-band channel to do tunneling. In on-demand routing protocols such as DSR [9], once the wormhole is established, the only route that can be found is the wormhole. Other legitimate route requests will be suppressed since the route request via wormhole typically reaches the destination faster, and presents fewer hops, causing

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

rushing attack [58] in this case. Another property of wormhole is that the attacker can initiate a valid message without bothering to provide the valid authentication information by replaying the old message overheard before. This attack in geographic routing is not as difficult as in topology-based routing because the location information in the packet effectively helps the receiver to detect the potential tunneling based on the basic principle that the last hop sender is supposed to be within its transmission range.

Resource exhaustion: Excessive packets could be injected into the network to use up its resources. This attack assumes a powerful attacker with sufficient energy and it will be especially severe when applied to packets with broadcast property or cryptographic verification requirement. Excessive broadcast packets introduce severe traffic burden to the network. Cryptographic verification requirement for a specific node also causes undesirable host resources consumption such as CPU and battery. In geographic routing, no network-wide broadcasting messages are involved, so cryptographic verification torture stands out as the main concern of resource exhaustion attack. Most likely, an attacker will excessively sends out hello messages with junk authentication data, signatures, and overwhelms other neighbor nodes by signature verification. In addition, packets requiring end-to-end verification are another source of threat from denial of service by cryptographic verification torture.

Routing loop: This attack can also happen in geographic routing. An attacker can spoof as other nodes to disseminate false location information. For example in Figure 3.6, the malicious node M moves into the range of A but out of the range of B to spoof as E and moves out of A to B to spoof as A . M keeps on refreshing the spoofed location of E and A , causing the traffic destined for D to a routing loop A, E, B, A .

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

Path interposition: The mobility capability boosts this attack since the attacker can move to some “advantageous” position to increase the chance of receiving packets from the target node. In topology-based routing, the attacker may put itself on the shortest path between the target nodes to achieve superiority in route selection. To reach this goal, the attacker has to know some topology information beforehand. In geographic routing, the attacker may interpose in the forwarding path by putting itself between the sender and the receiver, and as close to the sender as possible. The objective of path interposition is similar with that of a black hole attack. They draw traffic to the attacker on purpose, which facilitates tackling over the intended traffic for malicious intentions.

Neighbor puzzle: Since the forwarding is decided locally, the reliability of the local information is particularly important. It simply becomes the target of attacks. We reveal two potential usages of location spoofing in GPSR to make a neighbor puzzle attack. First, a selfish node may falsely present a close location to the sender in order to evade traffic. This is because a node with a close location to the sender tends not to be the closest neighbor in the sender’s range to the destination. An example is illustrated in Figure 3.7. The selfish node B informs a close location $(1, 2.1)$ to A and C to avoid the traffic.

Figure 3.6: Routing loop.

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

Second, the malicious node may present a further location than it really is to attract traffic. The black hole attack we discussed earlier is an example of exploiting this usage.

The Sybil attack, Wall blocking: Identity spoofing is the main means for routing loop attacker to succeed. If spoofing of network identities is exploited excessively, it may even cause denial of service to a certain victim. The attacker can simply fabricate enough nodes around the edge of the victim's radio range, leading all the traffic from that node to the forged nodes controlled by the attacker. Suppression of all packets denies the access of the node.

A Sybil attacker may present to the network multiple identities that may come from forgery and even compromised entities. It can control a substantial fraction of the system, thereby undermining redundancy, the traditional fault tolerance technique. The Sybil attacker can reach the same effect of a black hole by spoofing any other node with the location (1, 4) as in Figure 3.5. Since fabricating identities has no limit, the attacker can build a very large number of fabricated nodes, which could exhaust the memory of neighbor nodes, causing other legitimate nodes' information to be dropped. An example of an extreme case of the Sybil attack is to fabricate enough number of nodes around the edge of the transmission range of a neighbor node, forcing all the traffic from that node to the forged nodes controlled by the attacker. It could be a denial of service attack if

Figure 3.7: Selfish node.

Figure 3.8: Sybil attack and Wall blocking.

the attacker suppresses all packets. Figure 3.8 illustrates this attack. Nodes *B*, *C*, *D*, and *E* will not have the chance to forward packets from *A*. The virtual nodes look like a tight surrounding wall blocking *A*.

Cache poisoning: This problem is always raised due to the use of optimization techniques. In geographic routing, a simple optimization of location service is to learn location information of other nodes from all received or overheard packets. This may improve the overall performance of geographic routing but it brings about severe security problems. The attacker can disseminate packets with arbitrary location to fool other nodes. All attacks related to false location, especially black hole, may benefit from cache poisoning.

3.2.4 Attacks on location service

Location service aims at helping a sender determine the exact location of the receiver. Generally, it functions based on two parts: location update and location query. This is naturally the target for an adversary to launch attacks such as disruption of the location service, black hole, and resources consumption attacks.

In location update, a malicious node can spoof as other nodes to send forged update packets to their corresponding servers, or modify the location information in update

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

packets as required to forward. Such a location database poisoning attack may be exploited to launch black hole attacks since the location server will provide these forged locations to queries. Another more direct way that we have discussed not long before is that the malicious node can send a false reply claiming itself to be a location server or can simply modify the reply packet with a false location if it lies on the forwarding path. Furthermore, the location service may be disrupted if the update, query, or reply packet are maliciously dropped or misdirected to some other places without reaching the correct location server or the querying node.

Location servers are common nodes that are selected to serve others according to the publicly agreed algorithm. With limited memory allocation for such a service, they are vulnerable to memory consumption attacks. The attacker may push excessive junk location updates to some location servers, such that they could not serve other legitimate users since their buffers are exhausted by junk updates. For example, in DLM, a sophisticated attacker may put the nodes in a certain grid under great pressure of storing false location information by pushing to that grid enough fabricated update packets of different updating nodes whose location server is supposed to be in that grid. It is easy to find such updating nodes if the hash value of the identity of the node is the target grid. Another example is in GLS. An attack only needs to fabricate enough identities of nodes that are “farther” than a certain node to suppress it.

Furthermore, the location service usually has no access control. Every node is entitled to query for the location of the node that it wants to contact, including the malicious nodes. Since the location information is sometimes quite security-sensitive, unauthorized nodes are not supposed to have access to such information.

3.3 Countermeasures

We discussed many types of attacks in the last section. Sources of those attacks are from either internal or external attackers as we mentioned in Section 2.1. Towards preventing different types of attackers, we consider two major types of countermeasures in our work which will be discussed in the following subsections.

To simplify the discussion, we assume that every sender has the genuine location of the receiver beforehand, i.e. a “secure” location service in place. This assumption is helpful to restrict security problems in location service to a higher level without involving too many underlying delivery issues. We will discuss the secure location service issues in Section 3.4.

3.3.1 Authentication: external attack prevention

The external attacker is the direct source of all attacks discussed previously. This type of attacker is quite common in MANETs because the wireless channel enables any node with a basic radio transceiver to inject and intercept packets freely. Although external nodes may not be always malicious, and sometimes even helpful for the connectivity of the network, generally they tend to misbehave, and it is risky to rely on them for relaying packets. The link level authentication usually takes on the task of preventing external nodes from accessing the network. However, it generally introduces more computation overhead and longer delays since every node that a packet passes through will be involved in cryptographic operations. In comparison, in end-to-end authentication, only two communicating parties are responsible for the verification. We believe that it is always a balancing point in design considerations for a specific environment. It is preferable to use the link level authentication where external attackers are abundant.

The simplest way to realize the link level authentication is to use a global key shared by the whole network, and a typical message authentication code [13] for link level verifi-

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

cation. Only the message presenting a valid global key will be admitted into the network. The advantages of this scheme are simplicity and low computational cost for each host thanks to symmetric cryptography. Despite these advantages, it provides only limited security. Once the global key is compromised, the whole system is compromised. Furthermore, the internal attacker node is completely free from restriction for all attacks discussed.

A solution to this problem is to use $n(n - 1)/2$ shared key pairs instead of a single global key. Every pair of nodes in the network will have a shared key. In this scheme, the external attacker cannot participate in the network because it has to encrypt with a shared key with the node it wants to transmit a packet to. Unfortunately, this scheme using shared key pairs is not able to provide the broadcast authentication property to help to build up a verified neighbor list. In order to be verified by its m neighbors, a node has to know their identities in the first place, and sends m Hello messages with the corresponding shared key with each neighbor. This will introduce undesirable communication overhead.

Digital signature [20] is a powerful public cryptography scheme for broadcast authentication as well as providing unique security properties, such as non-repudiation. A node sends out a signed Hello message, which enables all receivers to verify the authenticity of the sender and the integrity of the message. Furthermore, the sender cannot deny having sent the message while the sender repudiation is possible in the symmetric scheme. This property serves as an important deterrent of sending false location. The main criticism at present for RSA signatures [33] is its relatively high computation cost for a low-end device caused by potentially large exponentiation. Researchers are now interested in ECC signatures [59] which are promising for lightweight wireless devices with limited computation capability.

We will discuss more authentication mechanisms in the context of geographic routing in the next chapter. With proper authentication mechanism in place, the external attacker cannot spoof as other nodes and send false location to launch black hole, routing

loop, neighbor puzzle, and Sybil attacks. Cache poisoning and resource exhaustion are also prevented since the external attacker can neither inject nor modify packets without being detected.

3.3.2 Post-Authentication: internal attack detection

Authentication, however, does not prevent the internal nodes from malicious behaviors. A legitimate node may be compromised due to a lot of reasons. One may consider a compromised node as an attacker with the knowledge of the secret information of one legitimate user. So the internal attacker will be able to use the compromised identity to participate in the network as a legitimate entity. If such compromised nodes exist, attacks like black hole, neighbor puzzle, and cache poisoning will come back into the picture because nodes are supposed to trust the location provided by a “legitimate” node according to the protocol. If several nodes were compromised, Sybil attack would be also enabled. Furthermore, the potentially abusing traffic could cause severe degradation of network performance and cryptographic torture.

Location spoofing, traffic abuse and forwarding misbehavior are three main mechanisms of delivering internal attacks, and they are extremely difficult to prevent even with cryptographic techniques. Redundancy techniques are frequently used to tolerate failures from unexpected attacks. As an example, exploiting multiple routes [41, 60] is commonly used in MANETs to enhance the reliability of data delivery. However, potentially undesirable network overhead and sequencing handling issues limit the practicality in civil or commercial applications. In the case of ineffectiveness of prevention mechanisms, detection becomes the major way to cope with internal attacks in geographic routing. We propose possible solutions based on detection methods to the corresponding problems as follows.

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

3.3.2.1 Location spoofing

Location spoofing means that the compromised node can advertise arbitrary location supposed to be trusted by others, which becomes the main cause of the attacking restrike such as black hole and routing loop, etc. It is desirable to have a mechanism that could determine whether the claimed location is genuine or not. One possible solution is to estimate the distance of the remote host by measuring the round-trip delay of a challenge message. The effectiveness of this approach is based on the principle that the remote host should not be further than the distance calculated by taking the round trip traveling time of a signal multiply by the nominal traveling speed of the signal, i.e. $d \leq t \times v$, where d is the distance between the verifying node and the remote host.

However, this approach is not able to limit the upper bound of the distance of a node. A malicious node is able to increase t by properly delaying sending back the response as long as the condition $t \times v \leq 2r$ is true, where r is the nominal transmission range. As a result, a malicious node can claim a farther position than its true one. In this case, selfish nodes exploiting nearer position cannot benefit from it while malicious nodes attempting to attract the traffic are not detected. Alternatively, if NFP [52], i.e. choosing the nearest node as the next hop, is applied as the forwarding strategy, this approach will not be able to identify the selfish node claiming a further position, but will be able to detect the node attempting to attract traffic.

Furthermore, appealing for the cooperation of neighbors is a possible extended solution of this approach. The effectiveness is based on the fact that a false claimed location tends to be inconsistent among several observers, i.e. a farther position presented to one party may be presented as nearer to other parties, and vice versa. However, the confidence of determination based on cooperation will decline due to potential colluding possibility.

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

A similar idea of applying signal traveling to estimate the distance was used in [61] to achieve the location-based access control typical in a wireless LAN. A proper configuration of several base stations is able to cover a non-regular physical area where users are authorized to access the network. Every user can request for location verification in the coverage of one base station which will measures the delay of the challenge-response exchange.

3.3.2.2 Traffic abuse

Another tough problem is traffic abuse, leading to the dramatic degradation of network performance or node resources exhaustion. As an example, in resource exhaustion attacks, injecting excessive messages with junk authentication data is especially hard to deal with. Nodes could be overwhelmed by performing considerable unnecessary cryptographic operations. We consider that a lightweight detection scheme would be possible to identify the malicious traffic and protect nodes from resource exhaustion or cryptographic torture. The basic idea is that if a node is under a denial of service attack, neighbors around the attacker should have experienced the anomalous traffic earlier than the victim. They can stop the attack before the target node becomes a victim.

This problem can be dealt with by introducing two boundary values: *Lower Bound* (LB) and *Upper Bound* (UB). LB and UB are traffic intensity levels that indicate the processing capability of the network and the target node. They serve as boundary markers for the appropriate responses to the suspicious traffic causing denial of service attacks. LB and UB are closely related to the type of traffic in the network. The traffic that requires authentication operations has a higher weight contributing to the boundary values. The common data traffic without the need of cryptographic operations like multimedia stream data has a lower weight, which is mainly related to the bandwidth resource of the node. Every node will mount a traffic monitor observing the different type of incoming

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

traffic from its neighbors. If the traffic intensity for certain destination exceeds LB , it indicates a potential threat of denial of service attack. One possible measure for the current node to take is to randomly drop some packets to regulate the traffic. Another possible response is to initiate a cooperative detection. The current node may collect and converge the information observed by other neighbors to confirm the malignance of its observed traffic. If the traffic for some destination exceeds UB , it confidently reveals an undergoing attack. The node should stop serving the traffic for a period of time and report the event.

As an example in neighborhood authentication, if an attacker is excessively sending Hello messages that require, for example, signature verification, neighbors of the attacker should notice the anomalous rate of Hello message from the attacker. They can ignore some of them, or even stop verifying them when UB is reached. For end-to-end messages with signatures such as location update messages, the immediate neighbor node of the attacker is able to detect the anomaly before the target is attacked.

This scheme does not lose its effectiveness even when colluding compromised nodes existing around the attacker because outer nodes around them will notice the anomalous traffic eventually. However, the farther away from the attacking point the node notices the anomalous traffic, the harder it is for it to contact other observers to converge the attacking information when LB is exceeded.

This traffic monitoring scheme is quite like the traffic policing on an ingress router in quality of service (QoS), but it has extra security considerations in mind.

3.3.2.3 Forwarding misbehavior

The common challenge towards securing any ad hoc routing protocol is to overcome forwarding misbehavior. Nodes claiming to be cooperative in the protocol could misbehave by dropping, modifying, or misdirecting packets as we have seen in Section 2.2.1. In addi-

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

Figure 3.9: Misbehavior detection in geographic forwarding.

tion to applying multiple paths [62] to mitigate the effect of delivery failures, misbehavior detection is another important method that has reduced network overhead.

A basic detection technique is to monitor the next hop's transmission. For example, A keeps on listening whether A 's next hop B has properly forwarded the packet to B 's next hop C . However, it cannot be directly used in geographic routing because it requires source routing protocols such as DSR [9]. The nodes in geographic forwarding can only decide which is its next hop towards the destination, but the basic detection technique expects to know at least next two hops along the path. However, this detection could be possible if the node could have two-hop neighbor list. For example, in Figure 3.9, S can decide whether I should forward to $I1$ because S knows the location of the two-hop neighbors $I1$ and $I2$. Furthermore, modification can be also detected by S .

However, detection errors may exist in such detection methods due to packet collisions or channel errors. Sophisticated decision model and response as proposed in the CONFIDANT protocol [38] are required to mitigate detection errors and discourage misbehaviors.

3.4 The Importance of A Secure Location Service

So far, we have examined many different types of attacks in geographic routing and discussed some important countermeasures based on the assumption that the sender has the knowledge of the receiver's location. In fact, the location service is another important component affecting the security of geographic routing. Obviously, if the sender could not obtain the receiver's location or the obtained location were not "correct" in the first place, the packet delivery would not be successful no matter how secure the forwarding mechanism is.

The simplest way to obtain the destination's location is to use flooding as used in the route discovery mechanism in on-demand routing protocol. Intermediate nodes are only responsible to propagate the request packet without the need to maintain any state or routing tables. On receiving the request, the destination will send back its location to the sender by geographic forwarding. The underlying security issues of this scheme are relatively easy to handle. End-to-end authentication with certain anti-replay mechanism would remove most of the security concerns.

The evident problem of flooding-based scheme is scalability. GLS [57] and DLM [15] are two important work towards a scalable location service. The basic idea of these two schemes is to introduce location servers or proxies for a node. Every node will have multiple location servers storing its location that are distributed in different areas or hierarchical levels. The designation of location servers is achieved by a certain server selection algorithm, which works in a distributed manner. All nodes are supposed to take equal responsibility of providing location service for the whole network. It is undesirable in ad hoc network that some special nodes are selected to serve all other nodes.

We proposed a secure location service [16], which will be discussed in the next chapter. The basic idea of the proposed scheme is to take advantage of redundant servers to mitigate potential location query failures due to either benign or Byzantine failures.

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

Furthermore, a majority voting principle is employed to achieve a high reliability of the obtained location.

3.5 Summary

In this chapter, we had a broad view of the security issues in geographic routing, and discussed some potential solutions to handle those problems. A proper link level authentication is effective to isolate external attackers, but incapable of handling internal attackers. We also provided a preliminary discussion of some potential techniques to detect malicious modification, forwarding misbehavior and anomalous traffic leading to denial of service. The security in location service is another important topic. Since there is no dominating location service available, the solution to protect location service might depend on the specific scheme used. Flooding-based location service is suitable for small networks while proxy-based location service is more scalable. In the next chapter, we will discuss our solutions for authentication in detail, and propose a secure location service based on DLM [15].

CHAPTER 3. A COMPREHENSIVE STUDY OF GEOGRAPHIC ROUTING SECURITY

Chapter 4

Location Update Protection for Geographic Routing

This chapter presents our efforts towards highly efficient authentication mechanisms that can combat attacks that we have identified in last chapter. The key challenge of the problem is to achieve an efficient scheme that can be affordable by MANET nodes while it does not compromise in security. We proposed three authentication schemes to protect the essential location update and query process in geographic routing, and we also carefully analyze the strength and limitation of each scheme.

However, in defending against a strong attacker model where nodes can be compromised, authentication mechanisms can hardly help as compromised nodes will have all the valid authentication information at hand. In the case, we do not consider the impact of updating nodes being compromised because it does not make sense that nodes make themselves unreachable by senders. And querying nodes should not be considered as compromised since by definition they wish to know the destination's location, i.e. the beneficiary of the service. Therefore, the main source of attacks is from location servers being compromised or nodes spoofing as location servers. We proposed a majority voting scheme over multiple query process to mitigate this impact in this attacker model, and

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

our simulation results show that the proposed scheme can tolerate much better than a common location service.

4.1 A Secure Location Service

Since obtaining the correct location of the destination is the very first thing for a secure location-based routing protocol, we propose a secure location service based on DLM [15] with the full length address policy to thwart the discussed attacks. We name the proposed secure location service SDLM, or Secure-DLM.

4.1.1 Assumptions

The proposed secure location service employs a simple scheme of geographic forwarding to deliver packets. It uses the digital signature scheme as the underlying cryptographic means for authentication due to its proved strength and popularity in the real life security systems. Furthermore, the digital signature provides an extra security property, non-repudiation, which is very useful for being an important deterrent of frequent misbehaviors in ad hoc networks.

Data or traffic confidentiality for the routing layer is not the major concern in our proposal. Traffic analyzers and privacy brokers are probably able to continue sniffing over the network, we target the prevention of malicious attacks on the routing infrastructure. We will discuss anonymity and location privacy issues in the next chapter.

We assume that there exists a key management service. Every legitimate node in the network has a valid certificate that is signed by a trusted third party such as certification authority (CA). Every node may obtain the certificate of the party it wants to contact through a certificate exchange protocol similar to Secure Socket Layer(SSL), which avoids piggybacking a certificate every time. If a node does not have the certificate of the other node but requires to verify its signature, it can first request that node for its certificate.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

A certificate contains mainly the ID of the node, public key of the node, time of issue, time of expiration, and the signature of the trusted party. We will discuss more about the key management schemes that can be applied to our proposals later.

4.1.2 Neighbor Verification for Geographic Forwarding

We have known that geographic routing is mainly driven by a reliable geographic forwarding strategy and a scalable location service which helps a sender to locate the target's location that is currently unknown or outdated. A typical proxy-based location service also depends on the underlying geographic forwarding to deliver protocol packets. Therefore, securing the geographic forwarding is always the first problem to consider, though later we will also see that geographic forwarding, to some extent, shares common features with location service.

As we can see in the last chapter, a variety of attacks are possible for geographic forwarding. For example, malicious neighbors may provide false location information and even fabricate some non-existent nodes to create routing blackholes and loops, etc. To protect against these attacks, neighbors with their claimed location are required to be authenticated before being inserted into a trusted neighbor list. If we assume that trusted nodes present their real locations and respect the protocol, attacks from external malicious nodes should not be possible. Any packets from spoofed and forged neighbors will be filtered and thus guarantee the integrity of the network state. Therefore, building a trusted neighbor list is the key task for a reliable geographic forwarding system.

For the reasons mentioned earlier, the digital signature scheme is employed to provide broadcast authentication for neighbor verification. Broadcast authentication requires that multiple receivers be capable of authenticating the message. Every receiver with the authentic public key of the sender can authenticate the message if a digital signature is

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

applied. Message authentication code (MAC) [13] is not suitable for broadcast authentication since it requires multiple receivers to have the same MAC key, which enables any receiver to forge packets and impersonate the sender.

To maintain a one-hop neighbor list, every node will periodically broadcasts a hello message containing its current location. We require that the hello message be attached with the sender's signature. For example, node A broadcasts a hello message which should be constructed as follows:

$$\langle [HELLO, id(A), location(A), timestamp]signature(A) \rangle$$

Sometimes an attacker may hold some hello messages that it overheard and replay them at a later time, causing an obsolete location notification. The timestamp in the message is used to prevent such a replay attack. Any receiver of the hello message will first verify the signature included in the message by using the sender's public key available in its certificate, which guarantees that the message came from the node as it claims to be, and that the message was not tampered with. If the certificate is not available at the receiver, the receiver can ask for it from the sender.

Furthermore, the receiver needs to check the location specified in the message since it is supposed to be within the range of itself. Even though the signature is valid, the claimed location may not be valid because of two possibilities: the sender is compromised or misbehaving, or there exists a wormhole. Since the invalid location may result from a wormhole attack, we cannot determine that the node included in the message is misbehaving. The message is discarded if the location is out of the range of itself.

After all the verification is completed, the neighbor is accepted as a trusted neighbor and will be updated to the trusted neighbor list. Every time a node executes the forwarding strategy, it will only send to the list of verified neighbors. Incoming traffic from unverified neighbors will be denied too. Thus, unauthorized nodes are isolated from the

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

network. Geographic forwarding should not encounter any external intrusions if certified users are always honest in the network.

4.1.3 Securing Location Service

A location service scheme basically involves location update and location query. Disruption of any part will potentially endanger the location service availability to senders who don't have the current location of their intended recipients. Our proposed scheme attempts to thwart all kinds of attacks threatening the availability of the location service, and it is mainly based on the Distributed Location Management(DLM) scheme [15], which has been briefly reviewed in the last chapter.

4.1.3.1 Authenticated Location Update

As we showed in the last chapter, location update is prone to masquerading and forgery attacks. If the location update is not protected in the first place, location queries from requesting nodes will not be able to have any valid destination locations from the location servers. Furthermore, there is a risk that the location server's resources for storing location may also be overwhelmed by fake updates. So, it is desirable for a location server to verify the authenticity of the source as well as the integrity of the update packet. For this purpose, each node should attach its signature to every update packet before sending out. An update packet should include the following fields:

$$\langle [UPDATE, server_grid, id, location, timestamp]signature \rangle$$

The *server_grid* field denotes the grid of the location server. The *timestamp* indicates the freshness of the location and prevents replay attack. When the location server receives an update packet, it first checks if the source should choose it as a location server

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

according to the server selection algorithm, and then verify the validity of the signature. The location server will accept the update packet only if both verifications pass. Figure 4.1 depicts a basic authenticated location update process for one update packet.

Figure 4.1: Location Update: A is updating its location server L_1 in grid P .

4.1.3.2 Authenticated Location Query

Location query is another vulnerable process threatening the integrity and the availability of the location service. A node initiates a location query when it does not have the location of the node it wants to communicate with. However, the query packet and reply packet may not reach their destination properly, or may be maliciously modified during propagation, or even come from an attacker. So, end-to-end authentication for both the query packet and the reply packet is required for a location query process. By having a proper authentication mechanism in place, we can achieve a basic security requirement, i.e. data integrity. This is also important to avoid unnecessary overhead imposed by serving either benignly or maliciously tampered packets. In addition, we consider unauthorized users should not be allowed to send queries for legitimate users to remove malicious purposes, e.g. advertising and spamming, etc. Thus, the end-to-end authentication of query packets also serves an access control purpose.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

In the proposed scheme, each query packet should carry with the querying node's signature to enable the location server to authenticate the query request. The query packet has the following fields:

$$\langle [QUERY, server_grid, querier_id, querier_loc, target_id, ts] querier_sig \rangle$$

Similarly, the corresponding reply packet includes the location server's signature and its grid information which ensures the querying node that the received location information is provided by the legitimate server in the authorized grid. The reply packet contains the following fields:

$$\langle [REPLY, server_grid, querier_id, querier_loc, target_id, target_loc, ts] server_sig \rangle$$

Figure 4.2 illustrates the procedure of one location query.

4.1.3.3 Majority Voting for Location Query

In fact, the location query in the original DLM may not succeed due to some benign failures. The location server may have left its current grid and the new location server

Figure 4.2: Location Query: B initiates a query to A 's location server L_1 for A 's location.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

has not been updated yet. A query or reply packet may be lost during transmission because of network congestion or dead-end topology. Furthermore, the location query may fail due to malicious attacks, such as packet dropping by some misbehaving nodes. A much more severe case is that a compromised location server may even provide false location information. Therefore, the original location query scheme will suffer from the potential node misbehaviors as well as from benign system failures. In order to tolerate different kinds of failures and misbehaviors, we proposed a multiple query scheme, named Majority Voting for Location Query (MVLQ). MVLQ takes the advantage of redundant location servers to enhance the availability of the query system and applies the majority voting principle to enhance the reliability of the obtained location information under a strong attacker model.

In MVLQ, a node initiates m queries to m location servers instead of querying only one server. The querying node discards all replies from invalid grids that are not supposed to have location servers, and then it selects the location with the largest number of votes. The process can be summarized as the following steps:

- (i) The querying node waits for a timeout to receive as many replies as possible.
- (ii) In the received replies, discard those from invalid grids by checking the *server_grid* field in the reply and verify the signature attached to the reply. The senders of those replies with valid signature but invalid grid must be misbehaving, which we can take positive actions against.
- (iii) The rest of the replies can be viewed as a triplet (grid, location, sender). Fill in Table 4.1 with the sender id of each triplet.
- (iv) Count all rows and columns with non-empty entries. Accept location i if $c_i = \text{maximum}(c_1, c_2, \dots, c_n)$. If several i exist, randomly select one.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Table 4.1: m server grids and n' different location in received replies

grid/location	1	2	...	m	sum of row
location 1					c_1
location 2					c_2
...					...
location n'					$c_{n'}$
sum of column	s_1	s_2	...	s_m	

- (v) If $s_i > 1$ then we can determine that at least $s_i - 1$ senders in column i are misbehaving since only one reply is expected from one server grid.

In our case, data in location update is supposed to be synchronized across all servers. The number of values for location should not be exceeding the number of location servers in a benign case. Therefore, the major voting should be successful if there is enough data from loyal servers.

MVLQ actually proposes a decision making process for querying nodes in the presence of some unreliable information. Therefore, its goal is to improve the key issue, i.e. reliability of location service, by using majority voting when making decisions. The key thing that MVLQ does is exploiting the redundant information in the routing scheme to mitigate the threat of misbehavior and to enable the majority voting in favor of information reliability. As a subsequent benefit, a higher availability of the service is achieved as well.

4.2 Security Analysis

In our scheme, digital signature takes care of both the end-to-end and broadcast authentication. The end-to-end authentication is for update, query and reply packets. The broadcast authentication is for hello packets. One distinct advantage of our scheme is that hop-by-hop authentication is avoided since it places much computation burden to all the intermediate nodes and introduces a significant end-to-end delay. However, the

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

disadvantage is that maliciously injected packets are not stopped from propagation since the authentication is only carried out at the destination. This problem is not as significant as in some on-demand protocols such as DSR, because no packets in our scheme will flood the network, which may cause denial of service.

Digital signature is the main authentication mechanism in our proposed scheme because it provides pretty good security properties such as non-repudiation as well as authentication and data integrity. However, since digital signatures usually rely on public key cryptography such as RSA, some researchers argue that such an expensive operation may be impractical for handheld devices with limited CPU capability and energy. An attacker may launch a denial of service attack by flooding excessive malicious packets to the nodes and overwhelming it with the cost of verifying the signature. However, we believe that digital signatures are feasible because of the following reasons:

- Sanzgiri et al. [1] tested the RSA signature operations on a laptop computer with an ordinary configuration, and showed that the generation and verification delay are 8.5ms and 0.5ms respectively. This is quite comparable to the typical packet processing delay, 1ms in AODV [1] for example.
- We believe with the advance of technology some dedicated chipsets will make the lightweight wireless devices capable of these operations. A good example is iButton [63], with the size of a dime and very low cost, which now can perform RSA operations within a second.
- Elliptic Curve Cryptography (ECC) [20] has shown its superiority in the deployment of security of handheld devices. ECC signature provides the same level of security of RSA signature with much less bits, computation overhead and key size.

Certainly, symmetric cryptography can be the alternative to the public-key scheme in terms of its efficiency. Message Authentication Code(MAC) is based on the efficient

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

symmetric cryptography and provides end-to-end authentication. There is no big change to substitute MAC for digital signatures in our scheme. The signature field changes to the MAC field, and nodes change to calculate MAC over the packet instead of signature. The disadvantage of MAC is that it requires shared secret keys, leading to the problem of the expensive distribution of a large amount of secret keys.

Assuming that each node in the network keeps its private key well and the public key cryptography is strong enough against cracking within a reasonable period, i.e. no node can forge signatures of others, the proposed secure location service is able to resist all external attacks that we have presented in section 3.2. The authenticated location update guarantees that the location server gets genuine location information of the node. Black hole attack using forged location is not possible since any modified or forged reply will be detected by the querying node through authentication. The proposed secure location service does not make use of location cache and therefore cache poisoning is avoided. In fact, all messages will carry the senders' signatures, which allows any node hearing the message to authenticate the source. The neighbor verification mechanism will maintain a trusted neighbor list, which will exclude unauthorized nodes from packet forwarding.

Due to the characteristics of MANET that we have discussed in section 1.2.2, internal attackers may exist. For example, in a hostile environment, such as a battlefield, some nodes could be captured, and some legitimate nodes may be compromised due to some reasons. Misbehavior from captured or compromised nodes is unpredictable and difficult to detect since they are able to provide valid authentication information. A certain number of compromised nodes may be also capable of collaboration. It is extremely challenging to thwart such a strong attacker model, however, the proposed MVLQ is able to mitigate the misbehavior caused.

With the basic authentication mechanism applied, compromised nodes cannot launch masquerading, modification, nor replay attack. However, the following misbehaviors are still possible:

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

- Not reply to a query as a location server
- Initiate a false reply as a location server
- Pretend to be a server and initiate a false reply to any non-server node that knows an ongoing query
- Packet dropping including update, query, and reply packets

MVLQ prominently enhances the availability of location service compared with the single query scheme because it is much more difficult for an adversary to block all location queries or replies. In Figure 4.3, location server S_1 is the nearest one to the querying node B , and the reply packet from it is unfortunately dropped because of node misbehavior on the forwarding path. In the case of the single query in DLM, the location query of B will fail. However, MVLQ still works because some location servers, such as S_2 and S_m , are not affected by misbehavior and can successfully send back replies.

Figure 4.3: MVLQ: B queries m location servers from S_1 to S_m

In the single query scheme, location server S_1 may be compromised and send a false location to B . Even though B received the reply, the false location included may lead to a black hole attack. MVLQ may also experience false replies, but false replies will not stop

B from obtaining the correct location if enough loyal servers provide the correct location, and the false location will be ignored after applying a majority vote on location. So, we can argue that MVLQ provides a higher probability of obtaining a correct location.

4.3 Performance Evaluation & Simulation Results

To evaluate the performance of SDLM and MVLQ, we implement the scheme in ns-2 [64], and conducted a few sets of simulations to show the performance results and compare it with the original DLM.

The objective of these simulations is not to examine the security strength of the proposal since security analysis discussed in the last section is considered more appropriate for this purpose. The focus of these simulations is to evaluate the protocol level performance of the proposal with new features and security mechanism added. By examining the whole picture of the impact the proposal makes in different performance metrics, it gives us a better view of the trade-offs affecting the system.

4.3.1 Simulation Scenario

Due to the lack of implementation of DLM in prominent network simulators such as ns-2 and GloMoSim, we implemented our scheme based on DLM with full length address policy in ns-2 under the help and clarification of the original author. The ns-2 simulator is actively used in network research and offers high fidelity as it includes a full simulation of the IEEE 802.11 physical and MAC layers. CMU also developed wireless extensions [65] for ns-2 to provide wireless support. In our implementation, GPSR greedy mode is employed as the packet forwarding agent for the location service.

The nodes are placed at uniformly random locations in a square universe $700\text{m} \times 700\text{m}$. The smallest DLM grid has 175 meters on one side. The total number of location servers for a node is 4. Each node moves using a random waypoint model [66]. The node

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

chooses a random destination and moves towards it with a constant speed uniformly chosen between zero and the maximum speed. When it reaches the destination, it pauses for a specified time and then repeat the same process. In our simulation, pause time is 10 seconds. We evaluate the following performance metrics during the simulation:

- (i) Query success ratio: The query success in our context will have two levels of meanings, i.e. availability and reliability. To achieve a query success, the node who initiates a location query needs to receive at least one reply to the corresponding query. However, due to active attacks, a query will only succeed when the querying node has a way to accept a genuine location reply. The two sides of the location service will be examined respectively in the simulations.
- (ii) Normalized packet overhead: This is the average number of protocol packets forwarded and originated for each successful location query. DLM and SDLM both have four types of protocol packets: hello packets that are generated every three seconds but not forwarded, location update packets that are also periodic but require forwarding, and location query and reply packets that also require forwarding.
- (iii) Normalized byte overhead: It is computed as the average transmitted bytes of protocol packets for each successful location query. Protocol packets also include all four types, and are counted at each hop as in normalized packet overhead.
- (iv) Average query delay: This is the average time from sending out a query to receiving the first corresponding reply, i.e. the average delay for one successful query.

The main parameters in the simulations are summarized in Table 4.2.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Table 4.2: Simulation Parameters
Scenario Parameters

Network Area	700 m × 700 m
Grid Size	175 m × 175 m
Maximum Node Speed	10, 15, 20, 30, 50 m/s
Pause Time	10 seconds
Number of Nodes	20, 30, 40, 50, 70
Nominal Radio Range	250 meters
Location Query Rate	1 query/15 seconds
Raw Physical Link Bandwidth	2 Mbps

DLM Parameters

Location Update Interval	20 seconds
Location Query Rate	1 query/15 seconds
Number of Location Servers for a Node	4

Cryptographic Parameters

Digital Signature Size	16 bytes
------------------------	----------

4.3.2 Results and Discussion

4.3.2.1 Performance Results

The simulations only involve the location service and the greedy forwarding, without any data traffic. Each node in the network initiates a location query to a random destination every 15 seconds over the course of the 300 second simulation, starting at 10 seconds.

Figure 4.4 shows the query success ratio as a function of the total number of nodes in the network. In this simulation, no modification and fabrication attacks are involved, and hence a query in both schemes with and without MVLQ will succeed if at least one location reply is received. Thus, we consider it more of an examination of service availability rather than the service reliability, which will be examined in other simulations.

Queries are not retransmitted in the simulations, so a success means a success on the first try. As discussed earlier, location query failures may be due to many reasons, such as server movement or the server is not being correctly updated because of delayed or lost location updates, or the query or reply packets were lost during propagation. Another

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Figure 4.4: Query success ratio as a function of the number of nodes. Nodes move at speeds up to 10 m/s.

problem of DLM is “void region”, which are grids without any nodes inside. In such cases, nodes whose server is designated in that grid will have no service. Also, packet loss may arise from a dead-end topology in the network. However, MVLQ takes the advantage of redundant servers and effectively mitigates the effect of all those problems, which presents a much higher success ratio than DLM. Furthermore, in Figure 4.4, there is a slight increase of success ratio with the increase of nodes since the higher node density experiences less “void region” and dead-end topology.

Figure 4.5 shows the average delay for each successful query. Unfortunately, the delay of MVLQ is significantly higher than DLM. We discuss some reasons that may contribute to this result:

- Since the location query is not retransmitted in the simulation when it fails, such a delay of one time query/reply exchange does not reflect the real delay for a successful query, that is, DLM may require more times of retransmission of the query in order to achieve one success while MVLQ nearly always does not need to

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Figure 4.5: Average query delay as a function of the number of nodes. Nodes move at speeds up to 10 m/s.

query more than once.

- In the simulation, all nodes are sending queries at a constant rate. Obviously, the traffic load of the entire network in MVLQ is much higher than that in DLM, leading to a prominent increase of delay during propagation in MVLQ. This can be greatly reduced if we apply a more realistic traffic scenario, for instance, 20 nodes out of totally 50 nodes in the network are querying for random destinations at a reasonable sending rate.

Furthermore, it is not an accurate metric to examine the query delay of MVLQ since MVLQ expects to receive more than one reply in order to extract the most reliable location. Therefore, a well-defined query timeout is desirable for MVLQ to wait for all expected replies. The timeout will be a constant query delay enforced to MVLQ, depending on the network size. Although the result in Figure 4.5 may not properly reflect the query delay, it does show that MVLQ suffers a higher delay compared with

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Figure 4.6: Query success ratio as a function of the node mobility in the network of 50 nodes.

DLM, and gives some idea of the baseline to define a timeout for MVLQ. The timeout should be above the MVLQ line in the figure with a reasonable extension value in which other replies are expected to receive. There is a possible approach to optimize the delay in MVLQ. Statistics on the number of the majority of replies can be captured after a period of time of running the system, which gives a threshold value for the current system to accept a reply. Later on, there is no need to wait for a whole query timeout. Whenever the node receives the threshold number of replies with same location information, it accepts it, which reduces the query delay.

Figure 4.6 shows the effect of the node movement speed on the query success ratio for 50 nodes. Although the location servers are more likely to be out of date as the nodes move faster, the nodes will also generate updates faster. Therefore, the query success ratio does not decrease significantly. The update traffic, however, grows as nodes move faster, which is indicated in Figure 4.7.

Figure 4.7 shows the normalized protocol packet overhead for each query success.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Figure 4.7: Normalized packet overhead as a function of the node mobility in the network of 50 nodes.

The result is generated from the same simulation for Figure 4.6. With the increase of node movement speed, nodes tend to leave their current grid more frequently. In DLM, whenever a node leaves its current grid, it will update all its location servers. Therefore, high mobility causes the update traffic to grow, and hence the packet overhead increases. It is always true that some overhead should be paid to mitigate the mobility effect. Figure 4.7 also shows that the packet overhead is quite close when node mobility is beyond 30 m/s. It indicates that in order to achieve the same success ratio, DLM needs to pay nearly the same packet overhead as SDLM with MVLQ due to more query failures caused by high mobility.

Figure 4.8 shows the normalized byte overhead for each query success. The result is generated from the same simulation for Figure 4.6 and 4.7. SDLM does not introduce any new type of messages, but requires messages to be signed by the sender for authentication. Thus, every control message contains an extra field of 16 bytes for signature, which unfortunately causes a significantly higher byte overhead in SDLM than in the original

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Figure 4.8: Normalized byte overhead as a function of the node mobility in the network of 50 nodes.

DLM. Multiple queries in MVLQ are another reason leading to the high byte overhead. In fact, there may not be a need to query all servers. We need only to query enough servers in order to get the desired level of reliability, which will minimize both packet and byte overhead.

4.3.2.2 Effect of Misbehavior

Simulations described in the last section only consider a benign network environment, where all nodes behave as expected. The simulations in this section try to examine the result by introducing some node misbehaviors. Misbehaving nodes are randomly selected at the beginning of the simulation, and carry out the following misbehaviors with probability set to 50% in the simulation:

- (i) Randomly drop when receiving an update packet.
- (ii) Randomly drop when receiving a query packet.
- (iii) Randomly drop when receiving a reply packet.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Figure 4.9: Query success ratio as a function of the number of misbehaving nodes in the network of 50 nodes. Nodes move at speeds up to 10 m/s.

(iv) Randomly initiate a reply when receiving a query as a server.

These misbehaviors can be distinguishable with packets getting lost accidentally because the packet dropping introduced into the simulation is intentional and controllable at a 50% rate, which is on top of the “accidental” packet loss as a benign network effect. For example, if a location server is compromised, one of the replies for two queries in average will definitely get lost, which is not necessary in a benign case.

Figure 4.9 shows the effect of node misbehavior on the query success. The graph presents a prominent downward trend of the success ratio for both DLM and SDLM with MVLQ. However, even when half of nodes in the network are misbehaving, SDLM with MVLQ still has a satisfactory success ratio, around 75%. On the other hand, half of the location queries will fail in DLM.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Figure 4.10: Reliability of location as a function of the number of compromised nodes in the network of 50 nodes in total.

4.3.2.3 Location Reliability

So far, we have seen that MVLQ can achieve a much higher service availability, and it shows a good resilience to misbehaving nodes in the network. In this section, we present the results of another set of our simulations that examine the service reliability, i.e. how reliable the received location can be.

In these simulations, we introduce some compromised nodes which are liable not only to suppress protocol packets but also to launch an active attack when they are in the role of a location server by providing forged location replies upon query requests. To avoid the higher risk of being detected, compromised location servers will try not to respond with forged location reply for every query received, but with a 50% probability that is used in the simulation.

Figure 4.10 compares the reliability of location for the proposed scheme with and without MVLQ. This metric counts for a query success in terms of reliable location when the querying node chooses a true location without being affected by compromised

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

location servers. However, it does not try to reflect the complete success ratio including availability because the location reliability is calculated only based on the cases that the querying node receives at least one reply.

We plotted three cases in Figure 4.10 to evaluate the location reliability:

- (i) The proposed location service without MVLQ, i.e. the single query scheme, where only the nearest server is requested. The reliability of location is determined upon receiving the location reply. A successful case is considered only if the location is from a royal location server.
- (ii) The proposed location service with MVLQ, where the querying node does not afford to wait for more replies. The reliability of location is determined upon receiving the first reply. A successful case is considered only if the location is from a royal location server.
- (iii) The proposed location service with MVLQ. The reliability of location is determined upon receiving the third reply. A successful case is considered if the majority location is from royal location servers. If no majority happens, the querying node will have to choose randomly among replies.

The first two cases compare in the sense that no majority voting is involved. Figure 4.10 shows that they have similar level of reliability in the received location despite of the number of nodes being compromised. MVLQ does not give an obvious advantage in achieving reliability in this case. Instead, it can be slightly worse occasionally because it increases the chance that the querying node can receive a forged reply first from other servers rather than the nearest location server.

In the third case of the figure, i.e. the querying node will wait for a few more replies, we can see MVLQ offers a higher reliability. This is because MVLQ outperforms in those

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Figure 4.11: Average end-to-end query delay for the number of replies with identical location which are genuine.

cases that a querying node receives a forged reply while it still has other two replies that might be from royal servers. Even though in those cases that a querying node receives a royal reply, MVLQ is unlikely to lose in choosing the right location with majority voting because it has one vote in advance to have a strong stand in voting, and the remaining votes can be equal out.

MVLQ does a good job under the individual attacker model. In theory, MVLQ can be challenged when compromised location servers start to collude, i.e. they can cooperate to gain advantage in majority voting by responding with same forged location. Although we consider colluding compromised nodes are very impractical in reality as they should be synchronized with interests, information, and even the on-demand actions on-the-fly, MVLQ can be successful as long as replies from royal servers are more than those from colluding compromised servers. We may see some clues in Figure 4.11 the cost we may have to pay to have enough royal replies.

Figure 4.11 shows the average delay MVLQ will experience in order to have specific number of replies that are from royal servers. We also plot scenarios with different number

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

of compromised nodes shown as legends, CN-5, CN-10, and CN-15. As we can see, the number of compromised nodes actually has little impact to the delay.

We do not include in this figure the typical delay required without MVLQ which has been evaluated in Figure 4.5. Generally, by using MVLQ we will expect a longer delay for queries, and to have a two-majority case, we will have around 17ms in delay as shown in Figure 4.11. As expected, the figure also shows an increase in delay in order to achieve more in genuine majority. To combat n colluding compromised nodes, we can also expect the cost of $n + 1$ genuine majority replies that we will have to pay for safety.

4.4 Extended Discussions

4.4.1 Location Update: The Key Protection

So far, we have proposed a relatively complete geographic routing system with the main focus on a secure location service. It defends against a variety of attacks including the tolerance of certain levels of misbehaviors in the network. In this section, we look at a generalized perspective for protecting geographic routing.

From the previous discussion we have learned that what drives a geographic routing protocol is basically two mechanisms: neighboring exchange and location service. A node regularly sends its current location to neighbors so that it could receive packets from them. It regularly updates its location servers so that it could receive packets from remote senders who may not have its current location. From this, we can see that neighboring exchange actually shares a similar role as location service, i.e. updating a certain set of nodes with its current location. The difference is that neighboring exchange happens within a local area while location service provides location update to remote nodes. Therefore, in our work, we would like to generalize it into a single problem, i.e. location update. For local exchange, we term it as *local location update* (LLU), and for the remote version in location service, we term it as *remote location update* (RLU).

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

As a consequence of a shared role, LLU and RLU will naturally be sharing similar types of threats and attacks towards the disruption of geographic routing. Attacks that we have discussed in the last chapter that exploit LLU vulnerabilities could be simply extended to target on RLU. As an example, the blackhole attacker who sends spoofed hello messages to a local victim may simply send a spoofed location update message with a forged location to a location server, which helps to mount a similar blackhole attack. The future traffic under attack will then be redirected to the attacker node.

We will not consider location query in our generalized location update problem. Actually, the location query procedure could be considered separately as a typical end-to-end security problem that could share the same solution with data delivery.

4.4.2 Alternatives of Local Location Update Protection

By following the idea for location update protection, we propose some alternative protection schemes for local updates in this section. Since LLU and RLU share most of the security problems and goals, we will focus first on alternative solutions, denoted as LLU- x , to LLU. These schemes might be further considered to be extended to RLU scenarios.

For completeness of our discussion, we include a summary of LLU-0 which is the scheme we applied in the proposed secure geographic routing protocol discussed earlier.

4.4.2.1 LLU-0

In LLU-0, each node periodically broadcasts an update message with its current location to its neighbors. The update message is digitally signed by the sender with its private key, and its certificate is also attached with the message. The main fields of LLU message include the message identifier, identity of the sender, current location of the sender, timestamp of the message about to send, a digital signature computed over all the earlier fields, and the sender's certificate. We denote the LLU message as $\langle \{LLU, id, loc,$

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

$ts\}sign, cert\>$. Each recipient of the message first verifies the attached certificate by using the public key of the trusted third party. If it is valid, it means the public key inside the certificate is genuine and is truly associated with the claimed sender, and could be used to verify the signature of the message. Furthermore, the timestamp included can be used to determine if it is a message replay or not. The location update will be finally accepted to update the recipient's neighbor table if there is nothing wrong in all verifications. In this case, a node without a valid certificate will be denied by the network since it will not be able to sign the update message properly. Any fabrication or spoofing of identities will not be possible either.

LLU-0 applies the digital signature scheme to make the solution quite straightforward. It provides most of the expected security properties, such as the authenticity of the sender, integrity of the location, and even sender non-repudiation, which is potentially useful as a deterrent of misbehavior since only the node with the corresponding private key can generate the signature. However, performing public-key cryptographic operations might be computationally expensive to low-end mobile devices. A node has to periodically sign its update messages, and has to verify all its received messages. It is also vulnerable to resource consumption attacks, where a malicious node injects a large number of fake LLU messages that need processing, and the computing resource or energy of innocent recipients may be exhausted in a short time. In fact, this problem exists in almost all cryptographic protocols that perform heavy cryptographic operations. Our defense solution is to mount an incoming traffic monitor, and each node will set a proper threshold value for the amount of incoming traffic volume that it can bear. Once the packet rate exceeds the threshold, it indicates that either a network exception or an attempt of resource consumption attack is taking place, and the node could respond accordingly to the event.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

4.4.2.2 LLU-1

LLU-1 targets the reduction of computation cost and the risk of potential consumption attacks when a pure public key scheme is applied. LLU-1 utilizes symmetric cryptography for authentication of update messages when it avoids the impracticality of using pairwise shared key. It is basically an authenticated key exchange approach based on key transport. The goal of LLU-1 is that every node generates a “group decryption key” within its own domain, i.e. its neighborhood. The group decryption key will be used for neighbors to authenticate and decrypt its update messages. We require a periodic beacon message to detect new neighbors and to remove “dead” ones. Each beacon message includes the sender’s certificate. The event of a new neighbor coming into node A ’s range triggers a direct group key transport of A . In this way, the group decryption key is delivered to the new neighbor so that it will be able to decrypt messages from A .

A neighbor table will be maintained at each node with each entry at least including the neighbor id, the status of key distribution, group key of this neighbor, location, and timestamp of location. An entry is added when an update message from a new neighbor is detected, and is deleted when no group key is timely distributed or when timeout happens on this neighbor due to the node failures or a broken link. Note that every node is able to receive messages and will maintain its neighbor table, but it will not be able to verify the update message and the source until it receives the corresponding group key from the source.

LLU-1 combines periodic beaconing and location update into a single update message, which reduces the required messages exchanged to save power and bandwidth. An example of this scheme is illustrated in Table 4.3. A and B are neighbors. E_k denotes the encryption operation with key k . gk_X denotes node X ’s group key. As a regular action, A broadcasts its update message to its neighbors. B finds that A is not in its neighbor table and starts to transport its group key to A . To securely deliver the key, B

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

extracts A 's public key from its certificate and encrypts the message after signing. On receiving B 's key transport, A is aware that B is also a new neighbor, and delivered its group key to B in a same way. By exchanging group keys, they are able to authenticate each other and be updated with fresh and reliable location of its neighbors. Although LLU-1 also involves public key operations, they are not performed periodically but are performed reactively when needed.

Table 4.3: Local Location Update Scheme 1

$A \rightarrow * : < \text{"LLU"}, A, \text{cert}_A, E_{gk_A}(A, \text{loc}_A, ts_A) >$
$B \rightarrow A : < \text{"Groupkey"}, B, E_{K_A}(\{B, gk_B\} \text{sign}_B), \text{cert}_B >$
$A \rightarrow B : < \text{"Groupkey"}, A, E_{K_B}(\{A, gk_A\} \text{sign}_A), \text{cert}_A >$
$B \rightarrow * : < \text{"LLU"}, B, \text{cert}_B, E_{gk_B}(B, \text{loc}_B, ts_B) >$

Another feature of LLU-1 is that the group key update for improving security is much easier. It is simply another round of key transport. However, in order to avoid incompatibility of different versions of the group key, sequence numbers could be introduced to identify the freshness of the specific group key applied or transported.

4.4.2.3 LLU-2

Traditional symmetric authentication is not able to provide broadcast authentication property as LLU-0 can, i.e. a broadcast message that can be directly verified by all recipients. If this property is available, multiple unicasts of the key distribution in LLU-1 could be avoided. We explore, in LLU-2, ways of applying TESLA [30] to achieve efficient broadcast authentication property based on symmetric cryptography. Each node using LLU-2 will generate a chain of keys in advance by hashing an initial random value consecutively. These keys are used in the reverse order as generated, and will be disclosed in a few time slots after use. An update message includes these fields, $< \text{"LLU"}, id, E_{tk_i}(id, \text{loc}, ts), i, tk_{i-1} >$, where E_x means the encryption operation with key x , and

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

tk_i is the i^{th} TESLA key. Each node in the network is supposed to send LLU messages periodically.

In order to correctly determine the sender's key disclosure, a recipient needs to know a few parameters that will allow it to construct a key disclosure schedule. It includes T_0 , T_{int} , and d , where T_0 is the starting time of the first time slot, T_{int} is the duration of a time slot, and d is the number of slots to pass before the key is disclosed. The very first commitment of the key chain is the last value of the hashing. Assuming that every node has reliable information on key disclosure schedule and the commitment of key chains of other nodes, the authentication at each receiver has the following two steps:

- (i) In order to authenticate the message, the receiver has to know the sender's key disclosure schedule, where it checks if the TESLA key tk_i used in the received message is disclosed or not. If the key is disclosed, the update will not be accepted. Otherwise, the message is buffered for future verification.
- (ii) Authenticating the disclosed key tk_{i-1} requires the commitment of the sender's key chain, and certain early-verified keys of the sender's key chain. With the commitment, TESLA keys are completely self-authenticated, because hashing any disclosed key a certain number of times is supposed to be equal to the commitment (recall that TESLA keys are used in the reverse order of the chain generated by consecutive hashing). The authenticated key could be used to verify the old update message buffered. Furthermore, the disclosed key can now be used as new commitment to replace the old one.

By using TESLA, LLU-2 allows nodes to efficiently generate and verify MACs over the periodic location updates. But LLU-2 presents another problem due to the temporal effect of TESLA for broadcast authentication, i.e. the node will always have a list of neighbors with old location information authenticated. How old is the location is tightly

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

dependent on the frequency of location update as well as the key disclosure schedule. In a low mobility environment, it may have little impact. Our solution to this issue is that the sender could anticipate its future position based on its current speed and direction, and send the update message with the anticipated future location after key disclosure time.

The location inaccuracy incurred by using TESLA is the major concern of routing performance degradation and non-optimal path selection. However, movement prediction capability should reduce the inaccuracy to a large extent. And we believe that movement prediction should not be a difficult job, especially when it is only predicting into a several-seconds future. In this case, every node will have a reasonably accurate and authenticated position estimate of its neighbors.

As readers may have noticed, the LLU-2 scheme we discussed above has an assumption that the key disclosure schedule and the key chain commitment are the prior knowledge of every verifier. This means that TESLA requires a prior receiver setup, i.e. these critical information has to be securely distributed to all expected receivers. It is not a good idea for key schedules of all nodes to be fixed throughout the network lifetime and pre-distributed to all expected receivers, since the storage requirement is similar to pairwise shared key which is linear to the network size. Therefore, LLU-2 also employs digital signature to secure the distribution of key disclosure schedule. However, LLU-2 does not require the node to sign messages periodically, the signature generation for the key disclosure schedule and key chain commitment could be an offline operation.

4.4.2.4 Security of LLUs

We shall discuss the security of all schemes based on the “outsider-only” adversary model, i.e. only legitimate users have valid authentication secrets like shared secrets or private keys of their certificates, and legitimate users are cooperative as specified by the protocol.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

We do not consider compromised nodes in this analysis. It is a separate topic requiring different detection or tolerance techniques.

Schemes that we have discussed so far can thwart all attacks we mentioned in Section 4.4.2, because without valid authentication data, attackers are not able to masquerade as other nodes nor to disseminate false location information. In addition to the authentication and data integrity that LLU-0, LLU-1, and LLU-2 can provide, some applications may require the protection against unauthorized eavesdropping, especially when location information becomes sensitive for individuals or the entire task. In this case, confidentiality of LLU is required. LLU-1 has the inherent ability to provide confidentiality while LLU-0 and LLU-2 can be extended for that purpose. A direct extension of LLU-0 is to further encrypt the message with the public key of the receiver, but the sender needs to know the existence of its neighbors and their public keys beforehand. This will add on a few more beacon exchanges and encryption operations, and will result in large delays. Therefore, in terms of confidentiality the importance of using group key to encrypt messages as done in LLU-1 becomes obvious.

As we can see, all three proposed schemes assume that each node has a prior certificate which is typically issued by an external CA. We consider that it is inevitable, so most practical security proposals will more or less rely on a public key infrastructure or certificate scheme. Providing PKI support for MANETs is also another important research topic for MANET security. There are several distributed PKI schemes [43, 42, 41] proposed, which could be applied in our context. Capkun et al. [43] proposed a self-organized public key infrastructure where nodes issue certificates to each other based on offline trust relations. If a node wants to verify another node's certificate, it can find a chain of certificates starting from its own to authenticate it. The idea is similar to the PGP scheme. Luo et. al [42] proposed a fully distributed public key infrastructure based on threshold cryptography. All nodes in the network share a part of the system

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

private key, and any of k nodes can cooperate to serve as a CA for issuing and revoking certificates. The main difference in applying different prior security setup system is that they have different underlying trust relations in nature, which may fit into different applications or scenarios.

4.4.2.5 Performance analysis

We compare the performance of these three schemes in terms of communication, computation, and storage cost. Communication cost is represented by the number of messages involved in the protocol. Computation cost is represented by the number of different types of cryptographic operations.

All schemes require periodic local broadcast to update neighbors and need to adapt to the dynamic neighbor membership caused by node mobility. The frequency of sending LLU messages, f , is a very important factor affecting the cost involved in the link connectivity and freshness of positions. Obviously, it should depend on the node's movement speed s . The faster a node moves, the more frequent it should update its current location so that its neighbors can have the freshest information. However, with more transmissions, more power and bandwidth are consumed. For the power saving centric environment, f could be configured as the minimal frequency that satisfies connectivity and location freshness requirements. This is an optimization problem of the trade-off between power saving and forwarding performance. Given an optimized frequency, what really matters towards security is the potential computation overhead it incurs. We will further study the effect of f in the simulation.

LLU-1 requires extra multiple unicasts for group key updates to its neighbors. This multiple-unicast will not be periodic since the group key update is based on a new neighbor event trigger. LLU-2 requires another periodic broadcasting message to update its TESLA information including key disclosure schedule and key chain commitment. Although LLU-2 has two periodic broadcasting messages that include public key operations,

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

it has following advantages compared with LLU-0: 1) The sender does not need to compute the signature every time it sends an update message. The digital signature can be generated offline. 2) The receiver does signature verification much less often than in LLU-0 since it does not need to verify the message if it has the sender's TESLA information and has already authenticated them. However, the trade-off is that TESLA requires loose time synchronization and an extra storage of key chain and verification-pending messages, which is another source of overhead.

For the storage cost, LLU-0 only needs to store the neighbors' certificates, whereas LLU-1 only needs to store the neighbors' group keys because the neighbors' certificate is only useful when authenticating the group key transport. LLU-2 needs to store more than LLU-0 and LLU-1 and it includes the neighbors' certificates, key disclosure schedule, last key chain commitment, and the buffered update messages, though it is stored temporarily.

The basic operation and message formats of the three schemes are summarized in Table 4.4.

Table 4.4: Summary of Proposed Schemes

LLU-0	$\langle \text{"LLU"}, \{id, loc, ts\}sign, cert \rangle$
LLU-1	$\langle \text{"LLU"}, A, cert_A, E_{gk_A}(A, loc_A, ts_A) \rangle$ $\langle \text{"Groupkey"}, B, E_{K_A}(\{B, gk_B\}sign_B), cert_B \rangle$
LLU-2	$\langle \text{"Schedule"}, \{id, K_i, T_i, T_{int}, d\}sign, cert \rangle$ $\langle \text{"LLU"}, id, E_{tk_i}(id, loc, ts), i, tk_{i-1} \rangle$

4.5 Summary

In this chapter, we proposed a secure location service, which isolates unauthorized nodes and provides authenticated location update and query with reliable packet forwarding. To overcome system failures and compromised nodes, we proposed Majority Voting for Location Query to enhance the availability and reliability of obtaining a correct location.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

A secure location service is not limited to the use in location-based routing. It can also be used in any location-based application that relies on the accurate and correct location information.

Although a secure location service seems very essential to secure a location-based routing protocol, we find that “location update” is an equally important part of geographic routing. Thus, the protection for both local and remote versions of location update become the key security issue. We discussed a few alternative schemes for local location update protection, and analyzed their strengths and weaknesses.

In the next chapter, we will address a different aspect of geographic routing security, which is the location privacy of the nodes in a location based routing scheme.

CHAPTER 4. LOCATION UPDATE PROTECTION FOR GEOGRAPHIC ROUTING

Chapter 5

Location Privacy Preservation in Geographic Routing

This chapter addresses another important security issue, i.e. location privacy, that has not yet been brought up by the research community in MANET security. Our work is the first effort to pose and to address this issue for geographic routing.

Preserving location privacy proves to be especially challenging in geographic routing because location information is essential to this type of routing and has to be in clear text so as for the geographic forwarding process to work, and giving up on using location information is obviously not a solution to the problem.

However, we considered this problem from an innovative perspective, i.e. the location itself should not be considered sensitive to privacy until it is associated to a subject. We overcame the coupling of location and identity in three critical components to make it a complete location privacy aware geographic routing protocol. Our simulation results also show that to preserve location privacy, we will not compromise in performance loss.

5.1 Introduction

Routing decisions in geographic routing are made by measuring the geographic superiority among neighbors. The attempt to utilize available location information helps to make localized decisions that are essential to the scalability of the network [67]. Although location usage promises enormous benefits in terms of routing efficiency, it is very hard for this class of routing protocols to be further applied into real life environments. Most of the existing works assumed an environment free from privacy concerns, and focuses on the routing performance by making the best use of any type of location information. This excessive and uncontrolled usage of location information potentially raises severe concerns of privacy in mobile and pervasive environments [68].

The first thing worth paying attention to is the scale of the privacy problem. In daily life, people may not see the privacy implications in revealing their location except in special circumstances. You probably do not care if anyone discovers where you were at 10:30a.m. yesterday, but if all of your movements were recorded every 5 seconds with foot accuracy, you might start to see things differently. In addition, present-day networked computers make the observation, propagation and processing of information on-the-fly, and the memory of information can be potentially unlimited. So, the scale of this problem changes thoroughly in the context.

Specifically in ad hoc networks, most of the proposed geographic routing protocols [50, 53, 57, 15] require each node to periodically update its current location to its neighbors and in some cases to remote servers as well. There is no control over the exposure of node location, which potentially encourages the possible abuse. For example, an adversary may track the movement of an individual. By analyzing a history of tracking records, personal sensitive information such as health condition, social interest, political tendency, etc., can be easily revealed. Moreover, location sniffers are able to exchange their observation data freely or sell them to any interested parties, such as advertising

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

companies, to make profits. It should not be a surprise that some day you will receive tremendous amounts of advertisements related to your interests that you are not even aware of. In many cases, the consequences of information revelation is harmful due to possible abuse.

Although the problem is clear, preserving location privacy in geographic routing in ad hoc networks is a challenging task. The expected solution is not only required to prevent location sniffing from outside of the network, but also from the internal attackers or the inside. The absence of a proper centralized administration in ad hoc networks also means that there is no pressure of investigation and legal pursuits for information leaking. In centralized wireless networks, such as cellular networks, the problem of location exposure also exists, but typically users have a privacy agreement with their operators. Users trust the service because their location is only collected by base stations rather than by any other peer user or outsider.

However, the problem is that it is not practical for every node in the ad hoc network to enforce privacy policies. Traditional privacy preservation approaches [68, 18] based on centralized control are not suitable in this context. Security solutions for content privacy such as IPSec [26] are also not applicable because routing information is not within the scope of protection of IPSec. Another approach using link level encryption for location imposes a severe computational burden to the network while it only prevents external eavesdroppers. The research community thus far has very little work on the privacy issue in ad hoc networks despite a considerable number of secure routing protocols [29, 32, 1, 31] have been proposed. The most related work is ANODR [69] proposed by Kong and Hong. ANODR is an anonymous on-demand routing scheme, and it provides route untraceability by using route pseudonymity. ANODR protects location privacy naturally due to its strong anonymity.

Since we are addressing issues in location-based routing, to restrict or stop using location information is not a solution at all to the problem. We expect to address the

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

location privacy issue without compromising on the utilization of location to improve routing efficiency. Two major proposals are discussed in Section 5.2 and 5.3 respectively.

5.2 Anonymized Geographic Ad Hoc Routing

The basic idea in our scheme is that location with identity is much more valuable than location itself. Therefore, the unlinkability of location to its identity could achieve a certain level of location privacy in the sense that the adversary with only location information cannot derive the identity of the subject who is at that location. In fact, certain locations may have indications of the identity of the subject, e.g. the location of the dean's office. However, we will only consider the general case in this dissertation, and we assume that location itself is not enough to derive the identity of its subject.

The location privacy problem must be addressed at multiple network layers to avoid a single penetration to lead to the compromising of the whole. However, our work will only focus on the routing design, particularly in the geographic routing scheme since it poses the major concern of the problem. We also assume that the upper layers are sufficiently able to take care of their own privacy issues. The organization of the discussion is as follows: Section 5.2.1 presents the general model of geographic routing, and discusses the privacy threats based on this model. Sections 5.2.2, 5.2.3, and 5.2.4 discuss our proposed scheme and describe three components towards the anonymity of geographic routing, which is followed by a security analysis in Section 5.2.5 and a performance evaluation in Section 5.2.6.

5.2.1 Threats Analysis

A few variants exist among different geographic routing schemes but the basic underlying concept of geographic routing remains unchanged. We summarize the geographic routing model in our work as follows:

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

- Local location update (LLU) - each node periodically updates its current location to neighbors along with its identity, which enables the building up of a neighbor table at each node.
- Remote location update (RLU) - each node periodically updates its current location with identity to remote location servers according to a specific location service algorithm, and reactively responds to location requests (the location server typically responds on behalf of it.)
- Location request (LREQ) - a source node who does not have the location of the intended destination initiates a LREQ message to the corresponding location server obtained by the location service algorithm. An LREQ message attaches the location and identity of the source so that the response of requested location could reach the requester.
- Data delivery (DATA) - during the data forwarding process, each packet attaches the location and identity of the destination so that geographic forwarding strategies could be applied and the intended destination could receive the data.

Based on the discussed geographic routing model, we can see that, a malicious node can keep on collecting the interested party's location through following ways:

- (i) Observe the interested node's location if it happens to be inside its radio range, or moves to be a relay/eavesdropper node over the path of the node's update, request, or data packets.
- (ii) Keep on making itself a location server of the interested node by following the location service algorithm applied, and accepting its remote location update.
- (iii) Keep on initiating location requests to the interested node's location servers.

- (iv) Collect the related information from its colluding nodes. Information from different sources could be merged.

As we can see, the location and identity is a basic doublet for distribution throughout the network so as to support the functionality of geographic routing. In the meantime, it is also the explicit source of threat to location privacy. The uncontrolled location exposure along with identity makes it a severe concern of privacy which we have discussed earlier. Malicious tracking and analysis of sensitive personal information can be performed easily.

To preserve the privacy of nodes in the network, we propose a privacy-aware geographic routing scheme by decoupling the location and its subject identity. The proposed scheme consists of three main components: anonymous neighbor table (ANT), anonymous greedy forwarding (AGFW), and anonymous location service (ALS).

5.2.2 Anonymous neighbor table (ANT)

Neighboring exchange is the main way of disseminating location information in geographic routing. Nodes build their neighbor tables by exchanging their location and identity in function. Maintaining an anonymous neighbor table (ANT) presents one of the biggest challenge in geographic routing. It is the essential component for supporting AGFW and ALS to be discussed in the next few sections.

5.2.2.1 Non-authenticated ANT

Every node in the network periodically broadcasts a *hello* message to indicate its existence and to update its latest position. The *hello* message is constructed like $\langle HELLO, n, loc, t_s \rangle$, where n is a pseudonym of the sender, loc is the current position, and t_s is a timestamp. n is randomly generated by the sender for each hello message, and the frequency of sending hello messages is typically based on the node mobility. A simple method to reduce the probability of n collisions in the neighborhood is by performing a hash over a locally

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

generated pseudorandom number and its identity to get n , denoted as $n = \text{hash}(pr, id)$. The hash function could be any “collision-resistant” hash algorithm.

Based on periodic neighboring exchanges, each node builds up its ANT with an entry like $\langle n, loc, t_s, t_o \rangle$, where t_o is the timeout for this entry. It is notable that a snapshot of ANT at a certain moment may have more than one entry for the same neighbor in this scheme, because the receiver of *hello* messages is not able to distinguish that the two messages are sent by the same neighbor, which is also a desirable feature we expect for anonymity. However, in order to take care of forwarding decisions involved with its old pseudonym, each sender of hello messages should memorize some old pseudonyms it generated. Due to the continuous timeout of table entries, it does not need to memorize too many but the two latest ones. Thus, if it receives a packet intended for any of its two latest pseudonyms, it should accept the packet.

However, multiple-entry for one neighbor may lead to ineffective forwarding decisions. For example, a node may select n_1 as the next relay node because n_1 is in the best position, but it didn't know that the node actually has moved to a worse location, indicated by the new pseudonym n_2 . To overcome this, our forwarding strategy has to go through a little modification. The forwarding decision should consider not only the position but also the freshness of the information. It is preferable to choose a fresher position rather than the best one in the ANT to improve the forwarding performance.

The scheme that we have discussed builds an AGFW-supporting anonymous neighbor table (ANT), which does not require a node to disclose its true identity. However, the authentication of neighboring nodes has not been considered yet. Potential spoofing attackers are not banned from the network and, for example, the attacker could forge a lot of hello messages with arbitrary pseudonyms to severely degrade the network performance and to mislead the forwarding direction. Therefore, we require an authenticated ANT, where a node needs to be authenticated to other nodes but at the same time, it should

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

not disclose its identity to any party including the communicating one. In general, providing security while maintaining location privacy is a great challenge. We will propose a solution based on Ring Signature.

5.2.2.2 Authenticated ANT based on Ring Signature

The authenticated ANT is based on Ring Signature [70] to achieve a $(k + 1)$ -anonymous neighbor table. We consider a neighbor table as $(k + 1)$ -anonymous, if and only if any neighbor in the table is indistinguishable from other k legitimate users. Therefore, the larger k is, the stronger the anonymity we have.

A ring signature scheme provides *signer-ambiguity* in the sense that the verifier is not able to determine the identity of the actual signer among a set of signers with size r . This set of signers is called a ring. There are two typical operations of a ring signature scheme: *ring-sign* and *ring-verify*. *Ring-sign* takes the message to be signed, all the public keys of members in the ring, and the private key of the actual signer as input to compute the final ring signature. The verifier of a ring signature could use *ring-verify* to check the validity of the signature but is not able to determine who actually generated it.

The basic operation of the scheme based on ring signature is illustrated in Algorithm 5.2.1. Node A borrows the required public keys $\{KU_1, KU_2, \dots, KU_k\}$ from certificates $\{cert_1, cert_2, \dots, cert_k\}$ of signers $\{N_1, N_2, \dots, N_k\}$ to *ring-sign* its *hello* message with its private key KR_A . All the involved public keys are also attached to the message in the form of certificates for the ease of verification at the recipient. In addition, to avoid correlation of two transmissions with the same set of signers, the sender should randomly select k public keys among all valid users. As one of A 's neighbors, node B can be sure that the sender is an authorized user in $\{A, N_1, N_2, \dots, N_k\}$ after signature verification, but it cannot determine who among them actually signed the message. By applying ring signature, ANT can achieve the important security property of authentication as well as $(k + 1)$ -anonymity.

Algorithm 5.2.1: AUTHENTICATED ANT(A, B)

comment: A simple example of AANT with nodes A and B

$A : m \leftarrow \langle HELLO, n, loc, ts \rangle$

$rsig_A \leftarrow \text{RING-SIGN}(m, KU_1, KU_2, \dots, KU_k, KU_A, KR_A)$

$A \rightarrow * : \langle m, rsig_A, cert_A, cert_1, cert_2, \dots, cert_k \rangle$

$B : \text{RING-VERIFY}(m, rsig_A, cert_A, cert_1, cert_2, \dots, cert_k)$

5.2.3 Anonymous greedy forwarding(AGFW)

AGFW achieves anonymous data delivery by avoiding the explicit specification of destination identity. It relies on an anonymously maintained neighbor table (ANT) to make routing decisions. The current AGFW scheme does not attempt to guarantee the packet delivery as it has no recovery mechanisms when a topology dead-end occurs. There is a variety of recovery mechanisms proposed in the literature [49] that can be used, but this will be dealt with in a future study of this scheme. At present, it suffices to assume that AGFW will not hit a topology dead-end.

The data packet header of AGFW is constructed as

$$\langle DATA, loc_d, n, trapdoor \rangle$$

where loc_d is the location of the destination, n is the pseudonym of the next hop relay, and $trapdoor$ is a value that can only be opened by the intended destination. By trying to open the *trapdoor*, a node could determine if it is the intended recipient of the message. This allows us to avoid explicitly stating the destination's identity in the message. One way to achieve the expected trapdoor function is to encrypt some data with the destination's public key,

$$trapdoor = KU_d(src, loc_s, tag_d)$$

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

where KU_d is the public key of the destination, loc_s is the location of the source and tag_d is some data like “Hey! You are the destination!”, which lets the node know that it is the target if it could properly decrypt the message. Here we assume that each node has a valid certificate signed by a trusted third party like a certification authority (CA), and that the source is able to know the destination’s certificate somehow, or it stores the certificate beforehand. Thus, the source will have a reliable public key of the intended destination.

On receiving a data packet, a node first decides if it is the intended next relay node by checking n . If n is not the pseudonym of the node, it will simply discard the packet. Otherwise, it will continue the forwarding process. It finds out the closest location in the neighbor table towards the destination, and transmits the packet to the neighbor with the associated pseudonym.

By following the above forwarding process, a data packet goes towards loc_d anonymously without disclosing any identity of the source, destination, or relays. However, there are two questions remaining, (1) how the destination receives the packet, and (2) how the forwarding process stops. In fact, a desirable feature here is that we do not require each forwarding node to waste computing resources on opening trapdoors for destination detection. The committed forwarder, who owns n , attempts to open the *trapdoor* only when it is in the last hop region. A node determines the last hop region by checking whether loc_d is inside its radio range. If the node successfully opens the *trapdoor*, forwarding stops. If not, it continues to forward the packet to a neighbor closer to loc_d . Once the node in the last hop region finds that it can neither open the *trapdoor*, nor have a closer neighbor towards loc_d than itself, it will make a local broadcast of the packet with n set to 0, which we call “the last forwarding attempt”. A pseudonym equal to 0 indicates to all receivers that they should try opening the trapdoor, and no more forwarding is required. As we can see in the discussed forwarding process, the destination

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

will be able to receive the data when it is either the forwarder in the last hop region or is one of the receivers of the last forwarding attempt. Furthermore, forwarding will stop when the destination either accepts the data or is unreachable.

All packet transmissions are local broadcasts so that it will disclose neither the sender's nor the receiver's MAC address. It achieves this by specifying a predefined broadcast address. In fact, the sender in AGFW will only know the next hop neighbor's pseudonym, which is what we want to achieve in ANT. The sender never knows which MAC address to specify for the neighbor nodes.

However, a node should not set its own MAC address either because of the possible linking to its location. We explain how this linking is possible: Since our protocol is not designed to be route untraceable, the eavesdropper can easily find out the last hop transmission and the next hop transmission of a packet by checking if the two transmissions have the same *trapdoor* information. Thus, if a packet is subsequently detected from MAC address A , the overhearing node can find out from its record history the last hop packet on the same route and the pseudonym n_A that was used. In this way, n_A can be confidently associated with A , and the location associated with n_A can be identified.

Another issue is that typical ad hoc medium access control protocols such as the IEEE 802.11 [3] do not provide broadcasting as reliably as unicast. To achieve reliable local transmission of packets, a network layer acknowledgment could be used. Once the current node receives the data broadcasted by the previous hop, it initiates an acknowledgment for the packet. The ACK packet is also locally broadcasted for anonymity, and it includes the information to uniquely determine the packet received. Furthermore, to reduce message transmission, the ACK packet can be piggybacked onto a data packet to be sent, so that it does not need to acknowledge one received packet at a time.

We summarize AGFW into some basic pseudocodes in Algorithm 5.2.2.

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

Algorithm 5.2.2: $\text{ONRECEIVEPACKET}(p\langle DATA, n, loc_d, trapdoor \rangle)$

```

procedure TRYFORWARD( $p$ )
   $N \leftarrow \text{CHOOSENEXT HOP}(ANT)$ 
  comment: ChooseNextHop returns a best suited pseudonym
  if  $N \neq me$ 
    then  $\begin{cases} \text{FORWARDTO}(N, p) \\ \text{return ( true )} \end{cases}$ 
    else return ( false )

main
  if  $n \in \{\text{pseudonyms}\}$ 
    then  $\begin{cases} \text{if } loc_d \cdot loc_{me} \leq \text{RadioRange} \\ \text{then } \begin{cases} \text{if OPEN}(trapdoor) \\ \text{then ACCEPT}(p) \\ \text{else } \begin{cases} \text{if TRYFORWARD}(p) = \text{false} \\ \text{then LASTHOPATTEMPT}() \end{cases} \end{cases} \\ \text{else if TRYFORWARD}(p) = \text{false} \\ \text{then STOP}() \\ \text{comment: Forwarding stops, recovery mode if applicable.} \end{cases}$ 
  else if  $n = 0$ 
    then  $\begin{cases} \text{if OPEN}(trapdoor) \\ \text{then ACCEPT}(p) \\ \text{else DISCARD}(p) \end{cases}$ 
  else DISCARD}(p)

```

5.2.4 Anonymous location service (ALS)

The last important component for a complete geographic routing scheme is location service which we have not yet discussed so far. In that case where the source node does not know the location of the destination, it should be able to retrieve it through a location service. However, to achieve an anonymous location service is a very challenging task as well. In this section, we propose a scheme based on DLM, a scalable location service proposed by Xue et al. [15].

In DLM, the network is divided into grids of the same size. Each node can determine some special grids, where its location servers are, by mapping its identity to it. Thus, the node identity and a certain set of special grids have established a fixed association with each other, which is publicly known. Each node will periodically update its location to its associated grids, and any querying node can initiate a location request to an associated grid of the required node to retrieve the location.

DLM provides an efficient way of managing location service, but without anonymity considered. The updater and requester will have to expose their location and identities to the location server in DLM. Our proposed anonymous location service attempts to dissociate a node's location and its identity but it does not provide the updater anonymity in terms of hiding its identity. The basic idea is that the updater will encrypt its location and its identity before sending it to the location server, and the potential location requester can retrieve it and decrypt it to obtain the location. The whole process of location updating and querying will not simultaneously expose the location and identity of any of the three parties. An example of our scheme is illustrated in Algorithm 5.2.3. For simplicity, only three nodes A , B and A 's location server S are involved in this example. Before we discuss how the scheme works, we introduce basic notations used in our illustration. $ssa(x)$ is the application of a server selection algorithm over value x . If it is

Algorithm 5.2.3: ANONYMOUS LOCATION SERVICE(A, B, S)**comment:** An example of ALS
$$\begin{aligned}
A &\rightarrow S : \langle RLU, ssa(A), E_{K_B}(A, B), E_{K_B}(A, loc_A, ts) \rangle \\
S &: \text{STORE}(E_{K_B}(A, B), E_{K_B}(A, loc_A, ts)) \\
B &\rightarrow S : \langle LREQ, ssa(A), E_{K_B}(A, B), loc_B \rangle \\
S &\rightarrow B : \langle LREP, loc_B, E_{K_B}(A, loc_A, ts) \rangle
\end{aligned}$$

applied on a node's identity, ssa returns the target grid where the node's location server is. We denote an encryption operation over message m with public key K as $E_K(m)$.

As we can see in Algorithm 5.2.3, node A uses its real identity to determine the remote location server but encrypts its location with B 's public key. Thus, any node other than A and B will not be able to read A 's location including the location server, although they do know where it is stored. Furthermore, A includes another component in the update message, $E_{K_B}(A, B)$, which is very important for the anonymity of querying nodes. This entry is used as an index for the location server to store updates. On receiving the location request from B , S is able to respond with the requested encrypted information by finding the entry with $E_{K_B}(A, B)$. Meanwhile, B does not need to worry about the exposure of its identity to sniffers, relays and the location server S .

Our proposed scheme avoids the explicit exposure of both location and identity in a traditional location service. However, the updating node has to identify all its possible senders and has to have one entry for every potential sender. Otherwise, some nodes may not be able to reach it. We consider this as a limitation of the proposed scheme. However, in practice, a node may not need to hide its identity or location all the time. A heterogeneous location update scheme may be more desirable. Once a node does not need privacy protection any more, it can switch to a normal location service in order to reduce the efforts needed for it to be accessed by potential senders.

Another problem is that the requester might have an exposure risk. Since the index part $E_{K_B}(A, B)$ is a fixed block of data, a sophisticated attacker may find a matching identity with a certain probability by collecting enough certificates or computing it exhaustively. An alternative scheme is that the requester does not provide the component $E_{K_B}(A, B)$, but the location server will return a set of encrypted locations that might be intended for different possible senders. However, as a trade-off for anonymity, the communication and computation overhead increases.

5.2.5 Security Analysis

The three proposed components ANT, AGFW, and ALS are expected to collaboratively realize anonymous geographic routing with no compromise of its functionality and performance. However, they are not designed to be route-untraceable. The path that a packet follows could be roughly estimated from the cleartext of locations in the packet since geographic routing basically follows a physically shortest path. The objective of this work is to dissociate location information from identity by anonymizing communications where location information has to be in cleartext. In AGFW, what a sniffer can observe is that packets are going towards certain locations. But it cannot determine who is sending to whom. Thus, location privacy could be protected in the sense that no node exposes its identity and location simultaneously.

The authenticated ANT achieves a $(k + 1)$ -anonymous neighbor table to support AGFW. The node sending *hello* messages can be authenticated by the verifier, but cannot be identified among a set of ambiguous signers. From the performance perspective, the scheme has to make a tradeoff between the anonymity requirement and the communication overhead in terms of number of bytes to be transmitted. The larger the set of ambiguous signers used, the stronger the anonymity the sender has, but with more certificates to transmit. To reduce the explicit communication overhead due to certificate

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

attachments, a sender may only specify identities or serial numbers of those certificates, and allow explicit request for required certificates in case the verifier does not have them. The number of explicit requests are expected to decline significantly after the network boots up for a period. Furthermore, in the scheme we assume that a node has enough valid certificates beforehand for ring signature, and so it must also have a certificate of the node that it is going to communicate with. In fact, this key management is another important topic of research, which is out of the scope of this dissertation. Our basic assumption in this work is that a legitimate node has its valid certificate obtained from an external certification authority, and this node might need to retrieve enough of the others' certificates for ring signature before entering the network.

Achieving a scalable location service is already one of the main challenges in the geographic routing research community. In our context, it is even more challenging to achieve an anonymous location service that coordinates before three parties (updater, server, and requester), and protecting their privacy at the same time. In the proposed ALS, an updater does not attempt to hide its identity but instead has its location encrypted. The requester will not need to expose its identity to the location server for retrieving location. Furthermore, location servers are also protected from being identified. As we have discussed, the main limitation of the scheme is that the updater is supposed to anticipate its potential senders in order to update the location servers properly. However, in a realistic application, nodes can apply heterogeneous location update strategies to adapt to its variable anonymity requirements.

5.2.6 Performance Evaluation

We implemented AGFW with the non-authenticated version of ANT to examine the performance of the new protocol behaviors. In our simulation, we did not incorporate ALS so as to focus our evaluation on the routing portion. Since ALS does not essentially

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

change the message exchange part of the protocol, the performance is expected to be similar to the original location service. With extra message bits and limited cryptographic operations involved, one might expect it to degrade a bit. The performance of the ring signature based ANT varies with the specific requirements of authentication and anonymity. A higher byte-cost is to be expected.

The two metrics we used for the performance evaluation are: (1) *Packet delivery fraction* - the fraction of the data packets sent out by sources that are delivered to destinations. (2) *End-to-end packet latency* - the average delay for a packet to be delivered from the source to the destination.

5.2.6.1 Simulation model

We use NS-2 with CMU wireless extension for our evaluation, which is widely accepted as the simulation environment for network research. Our implementation is based on the original codebase of GPSR [50]. The distributed coordination function (DCF) of IEEE 802.11 [3] is used as the MAC protocol in our simulations. Typically, a unicast transmission in IEEE 802.11 uses Request-To-Send(RTS) and Clear-To-Send(CTS) control packets as virtual carrier sensing for reducing the well-known hidden terminal problem. In addition, each data transmission is followed by an ACK.

AGFW requires data packets to be sent by local broadcasts in order to provide sender and receiver anonymity. Thus, without virtual carrier sensing, more packets may collide due to the hidden terminal problem. As we mentioned in Section 5.2.3, a network layer acknowledgment could help. In this case, the local broadcast employed in our scheme is equivalent to a unicast, except that 802.11 uses typical MAC addresses while AGFW uses identity pseudonyms for unlinkability.

In our cryptographic implementation, the size of the pseudonym n is equal to that of a typical MAC address. Therefore, we do not think that the pseudonym applied

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

Figure 5.1: Performance evaluation of the Anonymous Greedy Forwarding (AGFW).

in our protocol is an extra requirement in terms of packet size. For the *trapdoor*, we assume that public key cryptography support is available, and that there are no extra key exchanges. However, a lower cost symmetric encryption can be used instead if a proper key exchange scheme is in place. In our simulations, the size of the *trapdoor* does not exceed 64 bytes since it is obtained from the RSA [33] encryption with a 512-bit public key. A typical public-key encryption needs 8.5ms while the decryption needs 0.5ms for a portable computer processor [1]. Our simulations include a proper processing delay for where it applies.

Each simulation lasts for 900 seconds of simulation time. There are 50 nodes uniformly distributed in a network area with dimension 1500×300 . Each node has a nominal radio range 250m, and can move up to 20m/s with a pause time 60s whenever it changes its direction. We simulate 30 CBR traffic flows originating from 20 sending nodes.

5.2.6.2 Simulation results

Figure 5.1 (a) shows the packet delivery fractions of three schemes with the increase of the network density. We implemented a simple form of AGFW with no packet acknowledgment for comparison. Clearly, the delivery fraction of AGFW-NO-ACK is not satisfactory

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

due to the numerous packet collisions without ACKs and retransmissions. Furthermore, it gets worse when more nodes enter the network leading to more contentions and hidden terminals. AGFW with ACK has almost the same performance as the original GPSR-Greedy. It indicates that the change of protocol behaviors for anonymity requirements in AGFW does not affect its routing reachability very much.

Figure 5.1 (b) shows the comparison of average end-to-end latency of data packets. An interesting result we obtained is that the packet latency of both schemes does not make much difference when the network has a modest node density, i.e. when the number of nodes is no larger than 112 in our simulation. Intuitively, AGFW should have a longer latency due to its larger packet size and the cryptographic processing delay. However, GPSR-Greedy does not get more advantages here because: (1) The design of AGFW avoids the cryptographic processing overhead at every intermediate nodes. Only those nodes within the range of the destination are required to try opening the *trapdoor*. Therefore, a very limited number of nodes are affected by the processing overhead. (2) As we mentioned earlier, a typical 802.11 unicast involves a virtual carrier sensing by exchanging RTS and CTS, which contributes to the major part of the long latency of packet delivery in GPSR-Greedy. AGFW does not make handshakes before transmitting packets, so it could save quite a bit of waiting time compared to GPSR-Greedy. However, this saving is quite small because we expect more packet collisions in AGFW due to more hidden terminals with no RTS/CTS enabled, and the time saved in skipping RTS/CTS is partially spent in retransmitting packets and waiting for ACKs.

The results show a small difference in both schemes in terms of end-to-end packet latency. However, as indicated in Figure 5.1 (b), when the network density becomes high, GPSR-Greedy presents a significant increase of packet latency. This is because for a high density case, the traffic becomes relatively light, and GPSR-Greedy may suffer more latency with virtual carrier sensing.

5.3 Location Mixing for Preserving Location Privacy

We have proposed a location privacy-aware geographic routing scheme in the last section. It decouples the location information and the identity of its subject, and employs some cryptographic techniques to preserve location privacy. In this section, we consider an alternative approach which does not use any cryptographic technique for preserving location privacy. Therefore, two schemes are quite different in nature. The scheme to be proposed can be interesting when the network has very stringent requirements on computing resources, but relatively weak requirements on the level of location privacy to be achieved.

5.3.1 Introduction

Apart from the cryptographic approach of location protection, another straightforward and widely considered method is location mixing. In this approach, an entity mixes its accurate location with a larger area where there are many more other entities, and through the means the privacy of the entity's location can be preserved to some extent. In our case, if a node exposes only a mixed or rough location to its neighbors or location servers, it will largely improve its location privacy in geographic routing.

We may not have problems understanding how mixing location can benefit the preservation of location privacy, but we may have problems knowing how geographic routing can undergo a reduction of location resolution, and how location can be mixed for geographic routing which will not break the routing functionality.

Furthermore, the usage of location information in geographic routing now presents a conflicting goal. On one hand, the introduction of location is for making localized routing decisions, and hence provides better routing efficiency and scalability; on the other hand, location is now considered a sensitive piece of information, which should not be revealed without control.

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

Therefore, it interests us to find out if the lower location resolution in geographic routing is able to maintain the expected level of performance, and how the resolution could go to reasonably satisfy the specified performance requirement, as well as the location privacy that we can expect in the routing layer.

Before we examine the performance in simulations, we first propose a scheme of location mixing and discuss the related issues when low location resolution is introduced to the system. We also analyze the results in Section 5.3.4.

5.3.2 Resolution-Reduced Geographic Routing (RRGR)

5.3.2.1 Location Mixing Approach

To distinguish the proposed scheme with traditional geographic routing, we denote the proposed scheme as RRGR and denote the traditional one as TDGR.

To mix location, a node will map its true location into an area, which can also be called a mix zone. Only mix zones will be involved in geographic routing system and the accurate coordinates of the node are protected. However, the method of constructing a mix zone should not be arbitrary. It should have the following properties:

- (i) There should not be any explicit relationship between the true position and the mix zone, for example, constructing a mix zone by creating a circle with the node's true position as the center. In this case, the mix zone does not really mix the node's position.
- (ii) For consistency of applying routing information in the network, all network entities should apply the same method of constructing mix zones.
- (iii) The mix zones should not increase the difficulty of making forwarding decision.

We propose an intuitive approach for each node to create its mix zone by mapping itself to a geographic grid. The network area is divided into equally large grids, and each

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

node chooses the grid it currently resides as its mix zone. In this way, a node's true position is not directly exposed, and the resolution used in the routing system is reduced accordingly.

To accommodate the use of low resolution location, some of the protocol behaviors have to be changed. During the location update phase, only mix zone information will be periodically updated to neighbors or remote location servers. As a result, each node will be able to know a list of grids that some nodes reside, rather than know the exact location. For packet transmission, the source will only specify the destination grid information in the packet. The intermediate nodes will make the forwarding decisions based on the center of the mix zones of their neighbors. Potential sniffers including legitimate users can only know mix zones rather than the accurate location of the nodes.

Figure 5.2 provides an illustration of the mechanism in RRGR. Grey dots are where nodes really reside, while black triangles are “virtual” positions of nodes presented to the routing system. The forwarding node will measure the distances of all its neighbor grids to the destination grid in the packet, and choose the neighbor grid with the smallest distance to the destination grid as its next relay. This process iterates until the destination receives the packet, or when the destination is unreachable due to node mobility or network connectivity. RRGR has the same problem as greedy strategies, i.e. it may get trapped in a local maximum [49], and the forwarding node cannot find a better neighbor than itself to forward the packet. For GPSR [50], it has a perimeter mode so that the packet could get out of the location maximum and get forwarded to the destination.

5.3.2.2 Destination Grid Problem

We have discussed that in RRGR, each packet will contain the destination grid as the target location, and that the intermediate nodes will keep on forwarding the packet until the destination receives the packet. However, due to the introduction of the mix zone, the

Figure 5.2: Resolution-reduced greedy forwarding.

destination may become unreachable in RRGR while the delivery can still be successful in TDGR. For example, there can be more than one node in a destination grid, and they all have the same distance to the destination, and have the same chance to be chosen as the next forwarder. If one of the non-destination nodes in the destination grid receives the packet, it will never forward the packet any further since no nodes can be closer to the destination than itself. For TDGR, however, the packet contains the accurate location of the destination, and it will be further forwarded until it reaches the destination.

To avoid this unnecessary local maximum in RRGR, we enhance the geographic forwarding with destination detection: when the destination grid is within its radio range, the forwarder needs to detect if the destination node is inside its neighbor table. If the destination node is in the forwarder's neighbor table, it directly forwards the packet to it. Otherwise, the forwarder will forward the packet to another node in the destination grid. In fact, the probability that there is more than one node in a grid is large, and the probability will increase with the increase of node density or grid size.

5.3.3 Implementation & Simulation Results

The location mixing routing scheme allows each node to present only a mix zone instead of its accurate location to address the concern of location privacy. However, the reduced location resolution in geographic routing is likely to impact the routing performance. To

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

evaluate this, we conduct a set of simulations in NS-2 [64] with CMU wireless extensions. The prominent GPSR scheme is selected as the underlying geographic routing protocol. Based on Karp's [50] original implementation of GPSR, we incorporate the proposed RRGR scheme.

Simulation parameters similar to those in [50] and [71] were used for better comparison purposes. In the simulation, there are 50 nodes uniformly distributed in a network area with dimension $1500\text{m} \times 300\text{m}$. Each node has a nominal radio range of 250m, and can move up to 20m/s with a pause time 60s whenever it changes its direction. We simulate 30 CBR traffic flows originating from 20 sending nodes. Each simulation lasts for 900 seconds of simulation time.

We implemented two options to make forwarding decision in RRGR:

- (i) Use its current position to compute distance to destination.
- (ii) Use its last-reported grid to compute distance to destination.

In the original GPSR implementation, the node uses its most updated location to make forwarding decisions or to construct a planar routing graph. This is inconsistent of location usage among nodes because neighboring nodes only know the nodes' last updated and not its latest location. To overcome this, we allow a node to keep its last position, and use it to perform all forwarding decisions or to construct planar graphs until it updates its new location to its neighbors.

We also consider the second option because the forwarding decisions are made based on consistent data. The network also looks as if it was constructed with a consistent topology.

5.3.3.1 Packet delivery ratio

Figure 5.3 shows how the delivery ratio changes with the increase of grid size. Delivery ratio is the fraction of sent packets that are successfully received by the intended desti-

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

Figure 5.3: Performance vs location resolution

nations. Grid size equal to zero is actually the same as the original geographic routing protocol without reducing the resolution. We have four plotted lines in the figure. The “raw mode” and “last mode” are two set of simulations for the two forwarding options discussed earlier without destination detection. The “all-on mode” and “GPSR-allon” are two set of simulations with destination detection on for Greedy-only and GPSR.

The result of the “raw mode” and the “last mode” is not satisfactory since the delivery ratio drops constantly especially after the grid size reaches 50m. For this scheme of reducing location resolution, we have to pay noticeable performance degradation to achieve limited location anonymity. Whether the location usage is consistent or not also does not make noticeable difference in terms of delivery ratio. Based on this result, we can conclude that the probabilities of reaching a local maximum for the two options are similar.

For the “all-on mode” and the “GPSR-allon” mode, the delivery ratio maintains pretty well even when grid size expands to 150m, which indicates that a node can create a mix zone with size up to 150m with no significant degradation of the overall routing performance. However, after the grid size exceeds 150m, the delivery ratio significantly slashes to an unacceptable level. We can expect that the lower the resolution, the more severe the degradation of forwarding performance. With a larger grid size, the probability

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

Figure 5.4: Packet dropping causes

that more than one node will be in the same grid will be higher. In such cases, it is harder for the nodes to make forwarding decisions, and the packets are likely to be caught in a large number of local maxima.

Furthermore, the result shows that the greedy-only strategy is only slightly better than GPSR for smaller grid sizes, but degrades faster for larger grid sizes. This is because the perimeter mode in GPSR does not help to increase successful deliveries in smaller grid sizes but incurs extra packets overhead instead.

5.3.3.2 Packet dropping causes

In Figure 5.4, we examine different causes of packet dropping in the simulation. Packet dropping due to local maximum, TTL expiration, MAC transmission failure, no queue buffer, and routing loop are respectively denoted as “No route”, “Ttl”, “Mac-back”, “Ifq”, and “Loop”. We can see that the main cause of the decrease in delivery ratio is packet dropping due to forwarding failure, i.e. there are a lot of local maxima for the greedy-only scheme, where the node cannot find a closer neighbor than itself towards the destination. For GPSR, packets in the perimeter mode traveling through the network increase the network overhead and cause MAC layer contention. Many packets also cannot find a route to the destination as well.

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

Figure 5.5: Network diameter and node density effects (Greedy-only)

Figure 5.5 shows the effect of network diameter and node density on performance with the grid size set to 150m. Figure 5.5 (a) shows no evident effect of network diameter on delivery ratio, and Figure 5.5 (b) shows a slight improvement of delivery ratio with the increase in node density. This results from the fact that a higher node density will lead to higher neighbor density, which improves the forwarding selection.

5.3.4 Analysis & Discussion

Simulation results show that the use of low resolution location in geographic routing is able to maintain the routing performance well under certain conditions, which makes providing location privacy in geographic routing system possible. In this section, we explore the underlying reasons that allow us to reduce location resolution without significant loss of performance in the delivery ratio.

5.3.4.1 TDGR analysis under random networks

Since RRGR is a low resolution version of TDGR, it is important for us to understand what affects the delivery ratio of TDGR. To simplify the analysis, we only consider the greedy delivery of TDGR. We are not interested in any of the recovery mechanisms

Figure 5.6: Forwarding area of a node.

because they are just an improvement to the connectivity of the network.

There are a few factors affecting the success of a packet delivery, such as link condition, network traffic, existence of local maximum, etc. However, if a “local maximum” happens in the path of a greedy delivery, the packet will definitely fail to reach the destination. Therefore, the probability that a “local maximum” will happen is directly related to the delivery ratio.

Let us consider the probability of “local maximum”(LM) in TDGR, denoted as $P_{TDGR}\{LM\}$. For TDGR, LM happens if the forwarding node has no neighbor that is closer than itself to the destination. In other words, the greedy forwarding fails if no node is within the forwarding area(FA) of the current forwarding node. A node’s FA is illustrated as the shaded intersection in Figure 5.6.

To estimate $P_{TDGR}\{LM\}$, it is easier to first consider the probability that no LM happens to the data delivery. We may consider each delivery as a sequence of forwarding decisions made on a series of FAs approaching the destination. So, no LM for a packet delivery means that all of the FAs along the path are not empty. The probability can be

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

denoted as

$$\prod_{i=1}^d Pr\{N_{FA_i} > 0\}, \text{ where } N_{FA_i} \text{ is the number of nodes in } FA_i. \quad (\text{Eq. 5.1})$$

As we can observe in Figure 5.6, the more hops that a packet takes, the closer it is to the destination, and the smaller the size of the next FA will be. The smallest FA we can have, denoted as FA_{min} , is actually the intersection of two identical radio ranges with their centers on each other's edges, when the forwarder is as close to the destination as the radius of the radio range r . Obviously, the probability of FA_{min} having nodes inside it is smaller than any of the other FA_i . Thus, we can have the lower bound of (Eq. 5.1) as follows.

$$Pr\{|FA_{min}| \neq \phi\}^d \leq \prod_{i=1}^d Pr\{N_{FA_i} > 0\}, \text{ where } d \text{ is the path length in hops.} \quad (\text{Eq. 5.2})$$

Consider a network with an area of unity, where n nodes are uniformly distributed. The probability that there is no node in an area A is $(1 - A)^n$. Therefore, the probability of FA_{min} being not empty is $1 - (1 - FA_{min})^n$. And we get the low bound of the probability of no LM as $[1 - (1 - FA_{min})^n]^d$.

In fact, the size of FA_{min} can be determined since we mentioned that it is the intersection of two identical circles with radius equal to r and centers on each other's edge. Thus, we can derive the size of this area $FA_{min} = (4\pi - 3\sqrt{3})r^2/6$. d actually is a random variable since each packet delivery may follow a specific path that includes a specific set of relaying nodes and spans over different number of hops. Li et al. [72] derived the expected path length for a random network with random traffic pattern to be $\bar{L} = \frac{2\sqrt{A}}{3}$, where A is the network size. Based on this result, we derive the expected value of $\bar{d} = \frac{\bar{L}}{r} = \frac{2\sqrt{A}}{3r} = \frac{2}{3r}$. So, we can finally estimate the lower bound of no LM for TDGR as

$$[1 - (1 - \frac{r^2}{6}(4\pi - 3\sqrt{3}))^n]^{\frac{2}{3r}} \approx [1 - (1 - 1.2r^2)^n]^{\frac{2}{3r}} \quad (\text{Eq. 5.3})$$

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

Figure 5.7: Delivery ratio changes with node density.

From (Eq. 5.3), we can see that if n , i.e. the node density, increases, the final probability will increase accordingly. It indicates that the more nodes there are distributed in the network, the less possible that the packet forwarding will have local maxima, and hence there will be the higher connectivity and delivery ratio of the network traffic. This matches our simulation results in Figure 5.7.

An extra curve, called the LM bound, is also drawn in Figure 5.7. It gives the lower bound of the probability that no LM happens for the packet delivery. As we can see, the curve shows that the delivery ratio will increase with node density n . However, continuously increasing n does not always give an increasing delivery ratio. Constantly increasing node density leads to more routing control overhead and network congestions, which will cause the delivery ratio to drop at high node densities.

5.3.4.2 RRGR analysis under random networks

We have seen that the number of nodes available in the forwarding area is a direct factor for the maximum delivery ratio that can be achieved in TDGR. The situation, however, is different in RRGR:

- (i) Loss of density: With the increase in grid size, the number of nodes with different grid locations are decreasing because one grid is more likely to accommodate more

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

than one node. Thus, valid neighbors available to a node are decreasing too. To differentiate this from the commonly used node density, we call this the “grid density”, i.e. the number of grids in a unit area where at least one node resides.

- (ii) Uncertainty of FA: Not all nodes in the FA are eligible for forwarding, and forwarding nodes in certain areas within the radio range of the grid but outside of the FA could be eligible for forwarding in RRGR. If we denote the area eligible in TDGR but not in RRGR as A_1 and the area eligible in RRGR but not in TDGR as A_2 , the effective area we can have for forwarding in RRGR is $FA - A_1 + A_2$. However, the problem is that the estimating of A_1 and A_2 becomes very difficult since they are highly dependent on the grid size and also the direction of the destination.

The location mixing in RRGR results in the two changes above. Although the loss of density has a clear relationship with the grid size, we cannot easily estimate the effective FA linked with this grid size. Therefore, the uncertainty of the effective FA makes it hard for us to estimate a probability bound similar to what we have done in TDGR. However, determining the size of an effective FA can be a geometry problem, and it can be observed that the grid size does not affect the difference of $A_1 - A_2$ significantly. The analysis of TDGR actually tells that LM will be unlikely to happen if the node density reaches a certain level. It suggests that LM in RRGR will be unlikely to happen too if the grid density could reach a similar level. This is the reason why we consider RRGR’s delivery ratio will maintain well also within a certain grid size.

For the case that the grid size had increased to the level where the performance cannot be maintained, we believe that the increase of node density should be able to compensate for the loss of grid density. Therefore, a combined increase in both the node density and the grid size should be able to maintain the performance at an acceptable level. To validate this hypothesis, we conduct another set of simulations that examine

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

Figure 5.8: RRGR delivery ratio changes with the grid size and node density.

the delivery ratio with different node densities and grid sizes. As we can see in Figure 5.8, node density does help to maintain performance.

As expected, the network will have a limit for the grid density. The increase of node density will not always make improvements on delivery ratio. If the grid size is too large, the grid density becomes so low that the performance cannot be maintained no matter how dense the network is. The large grid size incurs too much inaccuracy in the destination location, so the packets will reach a position which is far from the destination. Furthermore, increasing node density will also increase the traffic overhead.

5.4 Summary

In this chapter, we addressed a very critical issue in geographic routing protocols, i.e. how to guarantee location privacy protection while location information is used to maintain the efficiency of geographic routing. We circumvent traditional methods like spatial and temporal cloaking and design an anonymous geographic routing for preserving location privacy. We propose three components working together to achieve anonymity of communication as well as to maintain the functionality of geographic routing. Furthermore, we explore an alternative way of preserving location privacy by reducing location resolution exposed. Our approach of mixing location proves to be able to maintain routing

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

performance within reasonable limits. The analysis also shows that the node density can help to maintain performance at low location resolutions.

CHAPTER 5. LOCATION PRIVACY PRESERVATION IN GEOGRAPHIC ROUTING

Chapter 6

Conclusion

We conclude our work by summarizing our major contributions to the area, and we outline some of the outstanding issues and possible solutions that can be taken up in our future work.

6.1 Summary of Research

The central theme of this thesis is the proposition of secure routing protocols for mobile ad hoc networks, in particular to propose a secure geographic routing method that is resistant to different types of security issues that we have investigated.

The amount of security research for ad hoc networks has so far been quite limited, although it is considered for a long time one of the most important issues to be solved before the deployment of this new networking paradigm. Based on our careful study of the literature, we identified one of the areas that is the most lacking in security research, i.e. geographic routing security. The importance of this class of routing in practical applications such as sensor networks presents our major motivation of this work.

Our contributions in this area can be summarized as follows:

CHAPTER 6. CONCLUSION

A comprehensive study of geographic routing security We had identified a number of attacks and threats in geographic routing, and accordingly considered some potential solutions to handle those problems. A link level authentication is considered effective to isolate external attackers, but is incapable of handling internal attackers. We also provided a discussion of some potential techniques to detect malicious modification, forwarding misbehavior and anomalous traffic leading to denial of service.

A secure location service The security in location service is very important for the whole system. Since there is no dominating location service available, the solution to protect the location service might depend on the specific scheme used. Flooding-based location service is suitable for small networks while proxy-based location service is more scalable. We proposed a secure location service based on DLM [15], which isolates unauthorized nodes and provides authenticated location update and query with reliable packet forwarding. Take into consideration the existence of system failures and compromised nodes, we also proposed Majority Voting for Location Query to enhance the availability and reliability of obtaining a correct location.

Local location update protection Although a secure location service seems to be a very essential part of a secure location-based routing protocol, we found that a secure “location update” is actually a fundamental building block of geographic routing. Thus, location update protection for both local and remote versions become the key security issues here. We proposed a few schemes for local location update protection, and discuss how these schemes can be extended to the remote version of location update.

Anonymized geographic routing protocol We addressed a very critical issue in geographic routing protocols, i.e. how to guarantee location privacy protection while

CHAPTER 6. CONCLUSION

location information is used to maintain the efficiency of geographic routing. We circumvent traditional methods like spatial and temporal cloaking and design an anonymous geographic routing for preserving location privacy. Based on the idea of dissociating the identity and location information, we proposed three components of a secure routing protocol to achieve anonymity of communication as well as to maintain the functionality of a secure geographic routing protocol.

Resolution-reduced geographic routing protocol Furthermore, we explore an intuitive way of preserving location privacy by reducing the location resolution exposed. Our approach of mixing location proves to be able to maintain routing performance well within reasonable limits. The analysis also shows that the node density can help to maintain performance at low location resolutions.

6.2 Future Work

Security problems in ad hoc networks are far from being solved. The research community is still very active in this area, and what we have done is to provide a limited contribution in a specific area of geographic routing security. We would like to outline some issues for further study which would hopefully drive the research in this area towards maturity.

Punishment Problem in MANET Misbehavior detection mechanisms can help nodes avoid the perceived malicious nodes so as to improve the throughput. However, misbehaving nodes currently do not receive any punishment for their misbehavior. On the contrary, they can freely enjoy the network service without contributing to it. Thus, more and more nodes will not have the incentive to cooperate, leading to a deadlock situation where no nodes want to forward packets for others and all will just wait there for service. Some form of punishment is therefore necessary to be applied to discourage

CHAPTER 6. CONCLUSION

those misbehaving nodes, so that all nodes are encouraged to cooperate and forward packets for each other.

The CONFIDANT [38] protocol introduces a punishment to misbehaving nodes for not forwarding packets to other nodes in the network. There are, however, two negative effects of punishment. The first one is caused by an imperfect detection mechanism. A node which was detected misbehaving may not really be misbehaving, so a cooperative node may be wrongly punished. The second problem is that a good node may have stopped forwarding packets to a suspicious or misbehaving node but it may be perceived by other nodes as misbehaving. This could be exploited by the attacker to slander good nodes that have identified the misbehaving node by simply flooding packets to them. In CONFIDANT, due to the spreading of such accusations, such false observations get carried to the whole network, and finally all nodes are not trusted by any nodes any more. In other words, a good node is discouraged from taking actions against the misbehaving nodes.

The cause of this problem is that the punishment action or enforcement is not being authorized to any single node to be executed. In a real life scenario, we will not think that the law enforcement department executing a penalty on law offenders is a kind of crime because the department is publicly accepted to do so. In addition, the first problem is prevented in reality because we have a long and stringent procedure to follow in order to ensure that the accused is truly guilty. Such a procedure is impractical in fast changing networks.

For future work, we can deal with the second problem in two possible ways:

- Find another punishment that discourages or isolates the misbehaving node but is publicly accepted.
- Find another way other than punishment to discourage or isolate the misbehaving node.

CHAPTER 6. CONCLUSION

Fault Tolerance based on Redundancy We have discussed in Chapters 1 and 2 that mobile ad hoc networks have sporadic connectivity in nature. With the dynamic changing network topology, the communication may experience connection interruptions due to the unexpected packet loss. From the security point of view, however, the byzantine faults resulting from non-cooperation or node misbehavior will be even more severe. While the network failures due to the dynamic topology are benign and possibly mitigated by protocol design, these network faults are malevolent and are very difficult to handle.

A detection-response system seems to be an indispensable mechanism to overcome this problem. However, the solicitation for the cooperation in detection makes the performance and effectiveness of the system questionable. Therefore, we believe that to some extent, a reliable and robust ad hoc network should have the ability to be resilient to faults on its own.

One of the considerations towards fault tolerance in ad hoc networks is to exploit route redundancy. Papadimitratos and Haas [60] have proposed some mechanisms to utilize the multipath features in on-demand protocols. For geographic routing, it is possible to exploit multipath features [62] too. However, we have to be clear in advance of the answers to some of the following questions:

- (i) How to specify the requirement of the fault probability for a specific network?
- (ii) How to quantify the fault probability caused by different reasons?
- (iii) How can redundant routes help the fault probability?
- (iv) What is the minimal number of redundant routes for the specified requirement for the fault probability?

CHAPTER 6. CONCLUSION

Key Management Up to now, our proposed scheme has an assumption that there exists a potential or external PKI for providing effective certificate management such as certificate issuing, renewal, and revocation. This subsection describes another important part of our future work that attempts to release this assumption.

Since its emergence in 1970's, public key cryptography has been recognized as one of the most effective mechanisms for security applications. Our proposed scheme employs digital signatures that is typically implemented with public key cryptography such as RSA. Effective management of digital certificates that contains public keys of the certificate holders becomes one of the key factors for the successful deployment of public key cryptography. Public key infrastructure (PKI), an infrastructure for managing digital certificates, was introduced for this purpose. The most important component of PKI is the certification authority (CA), the publicly trusted party that vouches for the validity of digital certificates. The success of PKI depends on the availability and reliability of the CA to provide certification service for entities or nodes in the network. PKI has been widely deployed for wired networks and some infrastructure-based wireless networks. However, it is a challenge to extend it to MANETs due to the distributed characteristics of MANETs, and the research on this area has been quite limited so far.

Our study on the current efforts indicates two radical security requirements for deploying PKI in MANETs: the confidentiality of the service private key and the availability of the certification service. Working towards these two goals, most of the current research show promising results but require further improvements. We intend to employ Threshold Cryptography [73] to achieve a distributed key management service with high confidentiality against compromised nodes and the availability of the service. With threshold cryptography, a system secret could be distributed to a set of nodes, and a threshold number of them could collaborate to provide services just as a centralized server does. The decentralized nature of such a scheme effectively avoid compromising the whole sys-

CHAPTER 6. CONCLUSION

tem when one server is compromised. Furthermore, availability of service is improved since the client does not need to rely on only one server for the requested service.

There is a strong adversary model, mobile adversary, that should be kept in mind. The mobile adversary model is first proposed by Ostrovsky and Yung [74] to characterize the attacker that temporarily compromise a server and then move on to the next victim. Under this adversary model, an attacker might be able to compromise all the servers over a long period of time. This would allow the attacker to reconstruct the private key. Proactive secret sharing scheme [75] could be used to address this adversary model.

Here we list some possible future work that will contribute to our design of the key management service:

- The very first question is what nodes should be chosen to share the CA functionality. It is worth careful considerations since it relates to the two security requirements mentioned above. A fixed selection of nodes for special tasks is not desirable for a fully symmetric ad hoc network and it will affect the flexibility of the network configuration, for example, when a designated node dies out or some new nodes join in. Furthermore, other nodes should be able to easily find these designated nodes.
- The certification service should have a “high availability”, and be able to tolerate different failures. It has been noticed that the service availability depends on the ratio of the number of nodes requested for the service coalition and the number of nodes that provide the coalition service.
- Propose an “efficient” and “scalable” secret share refreshing protocol. The secret share might need refreshing when a new node joins in. The share refreshing should be initiated in a periodic manner to protect against mobile adversaries. Furthermore, since potential communications for share refreshing may not be trivial, the efficiency and the scalability of the protocol should be also be considered.

CHAPTER 6. CONCLUSION

- Propose “efficient” and “scalable” communication protocols for certification services, which enables handling a large number of requests.
- There are some other important questions facing the designer. For example, what is the “policy” of the certificate issuing/renewal? How does a system “bootstrap”? The first question is non-trivial to answer and poses the root of the trust problem. The second question is also an important consideration for the design of key management service.

References

- [1] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in *Proceedings of IEEE International Conference on Network Protocols(ICNP)*, November 2002, pp. 78–89.
- [2] Bluetooth, "The Official Bluetooth Website." [Online]. Available: <http://www.bluetooth.com>, as viewed July, 2003
- [3] L. M. S. of the IEEE Computer Society, "Wireless LAN medium access control (MAC) and physical layer (PHY) specification." IEEE Standard 802.11, 1999 Edition, 1999.
- [4] T. G. Xydis and S. B. Wilson, "Security Comparison: Bluetooth Communications vs 802.11. white paper, bluetooth security experts group," 2002.
- [5] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proceedings of MobiCom 2001*, 2001.
- [6] S. Weatherspoon, "Overview of IEEE 802.11b Security," *Intel Technology Journal*, 2000.
- [7] W. A. Arbaugh, N. Shankar, and J. Wan, "Your 802.11 Wireless Network has No Clothes," in *Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks*, December 2001, pp. 131 – 144.
- [8] V. Karpijoki, "Security in ad hoc networks," in *Proceedings of the Helsinki University of Technology, Seminar on Network Security fall 2000*, 2000.

REFERENCES

- [9] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, Imielinski and Korth, Eds. Kluwer Academic Publishers, 1996, vol. 353, pp. 153–181. [Online]. Available: citeseer.nj.nec.com/johnson96dynamic.html
- [10] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, Feb 1999, pp. 90–100.
- [11] V. Park and S. Corson, "Temporally-Ordered Routing Algorithm (TORA) version 1: Functional specification. *Internet Draft, draft-ietf-manet-tora-spec-00.txt*," 1999.
- [12] Z. Haas and M. Perlman, "The Zone Routing Protocol (ZRP) for ad hoc networks. *Internet Draft*," 1998.
- [13] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," in *Request for Comments(RFC)2104*. Internet Engineering Task Force, 1997.
- [14] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on TCP," in *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, IEEE Computer Society. IEEE Computer Society Press, May 1997, pp. 208–223. [Online]. Available: <https://www.cerias.purdue.edu/techreports-ssl/public/97-06.ps>
- [15] Y. Xue, B. Li, and K. Nahrstedt, "A scalable location management scheme in mobile ad-hoc networks," in *26th Annual IEEE Conference on Local Computer Networks (LCN'01)*, 2001, pp. 102–111.
- [16] Z. Zhou, K. C. Yow, and S. Nandi, "A secure location service in mobile ad hoc networks," in *the Fifth IEEE International Conference on Mobile and Wireless Communications Networks*, 2003, pp. 274–277.
- [17] Z. Zhou and K. C. Yow, "Location update protection for geographic ad hoc routing," in *the 10th IFIP Conference on Personal Wireless Communications (PWC'05)*, August 2005, pp. 154–161.

REFERENCES

- [18] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *The First International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2002, pp. 31–42.
- [19] Z. Zhou and K. C. Yow, "Anonymizing geographic ad hoc routing for preserving location privacy," *International Journal of Network Security*, vol. 2, no. 3, pp. 210–218, 2006.
- [20] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 3rd ed., N. Jersey, Ed. Prentice Hall Press, 2002.
- [21] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread spectrum communication—a tutorial," in *IEEE Transactions on Communications, Col. COM-30, No. 5*, May 1982, pp. 855–884. [Online]. Available: citeseer.nj.nec.com/marti00mitigating.html
- [22] P. Kyasanur and N. Vaidya, "Detection and handling of mac layer misbehavior in wireless networks," UIUC, Tech. Rep., 2002.
- [23] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Worm-hole Attacks in Wireless Ad Hoc Networks," in *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*. San Francisco, CA: IEEE, April 2003.
- [24] H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," *IEEE Communications Magazine*, pp. 70–75, October 2002.
- [25] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," in *Proceedings of the 7th International Workshop on Security Protocols*, 1999, pp. 172–194. [Online]. Available: citeseer.nj.nec.com/stajano99resurrecting.html
- [26] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol. RFC 2401," November 1998.

REFERENCES

- [27] S. Kent and R. Atkinson, "IP Authentication Header (AH). RFC 2402," November 1998.
- [28] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP). RFC 2406," November 1998.
- [29] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," in *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, Sept. 2002, pp. 12–23, to appear. [Online]. Available: citeseer.nj.nec.com/article/hu02ariadne.html
- [30] A. Perrig, R. Canetti, D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," *RSA CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002.
- [31] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad Hoc Networks," in *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, 2002, pp. 27–31.
- [32] M. G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocol," in *Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002)*, September 2002, pp. 1–10.
- [33] R. L. Rivest, A. Shamir, and L. A. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [34] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.
- [35] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad Hoc Routing for Wireless Networks," in *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001)*, Long Beach, CA, citeseer.nj.nec.com/574412.html 2001.
- [36] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Mobile Computing and Networking*, 2000, pp. 255–265. [Online]. Available: citeseer.nj.nec.com/marti00mitigating.html

REFERENCES

-
- [37] L. Buttyan and J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WAnS," in *Proceedings of the First IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Boston, MA, USA, 2000. [Online]. Available: citeseer.nj.nec.com/article/buttyan00enforcing.html
 - [38] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confidant protocol: Cooperation of nodes — fairness in distributed ad-hoc networks," in *IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, 2002.
 - [39] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*. Denter, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121.
 - [40] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, "SPINS: security protocols for sensor netowrks," in *Mobile Computing and Networking*, 2001, pp. 189–199. [Online]. Available: citeseer.ist.psu.edu/perrig01spins.html
 - [41] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.
 - [42] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "Self-securing ad hoc wireless networks," in *IEEE Symposium on Computers and Communications*, 2002.
 - [43] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," in *ACM International Workshop on Wireless Security (WiSe'02)*, 2002.
 - [44] P. Zimmerman, "PGP user's guide," 1994.
 - [45] K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng, and K. Kim, "Highly reliable trust establishment scheme in ad hoc networks," *Computer Networks*, vol. 45, no. 2004, pp. 687–699, 2004.

REFERENCES

- [46] S. Capkun, J.-P. Hubaux, and L. Butty, "Mobility helps security in ad hoc networks," in *MobiHoc '03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM Press, 2003, pp. 46–56.
- [47] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, 1994, pp. 234–244. [Online]. Available: citeseer.nj.nec.com/perkins94highly.html
- [48] E. D. Kaplan, *Understanding GPS: Principles and Applications*. Artech House, 1996.
- [49] M. Mauve, J. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad-hoc networks," *IEEE Network*, vol. 15, no. 6, pp. 30–39, 2001.
- [50] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Mobile Computing and Networking*, 2000, pp. 243–254. [Online]. Available: citeseer.nj.nec.com/karp00gpsr.html
- [51] H. Takagi and L. Kleinrock, "Optimal transmission ranges for randomly distributed packet radio terminals," *IEEE Trans. Commun.*, vol. 32, no. 3, pp. 246–257, Mar. 1984.
- [52] T.-C. Hou and V. O. Li, "Transmission range control in multihop packet radio networks," *IEEE Transaction on Communications*, vol. 34, no. 1, pp. 38–44, 1986.
- [53] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," *Wireless Networks*, vol. 7, no. 6, pp. 609 – 616, November 2001.
- [54] F. Kuhn, R. Wattenhofer, and A. Zollinger, "Worst-Case Optimal and Average-Case Efficient Geometric Ad-Hoc Routing," in *Proc. 4th ACM Int. Symposium on Mobile Ad-Hoc Networking and Computing (MobiHoc)*, 2003. [Online]. Available: citeseer.ist.psu.edu/kuhn03worstcase.html

REFERENCES

- [55] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, "A distance routing effect algorithm for mobility (dream)," in *Proceedings of Fourth Annual ACM/IEEE International Conference in Mobile Computing and Networking (MobiCom)*, 1998, pp. 76–84. [Online]. Available: citeseer.nj.nec.com/article/ko98locationaided.html
- [56] Y. B. Ko and N. H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks," in *Mobile Computing and Networking (MobiCom)*, 1998, pp. 66–75. [Online]. Available: citeseer.nj.nec.com/article/ko98locationaided.html
- [57] J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris, "A scalable location service for geographic ad-hoc routing," in *Proceedings of the 6th ACM International Conference on Mobile Computing and Networking (MobiCom '00)*, 120–130 2000. [Online]. Available: citeseer.nj.nec.com/li00scalable.html
- [58] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *WiSe '03: Proceedings of the 2003 ACM workshop on Wireless security*. New York, NY, USA: ACM Press, 2003, pp. 30–40.
- [59] D. Johnson and A. Menezes, "The elliptic curve digital signature algorithm (ecdsa)," Univ. of Waterloo, 1999.
- [60] P. Papadimitratos and Z. J. Haas, "Secure data transmission in mobile ad hoc networks," in *Proceedings of the 2003 ACM workshop on Wireless security*. ACM Press, 2003, pp. 41–50.
- [61] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the 2003 ACM workshop on Wireless security*. ACM Press, 2003, pp. 1–10.
- [62] X. Lin and I. Stojmenovic, "Location-based localized alternate, disjoint and multi-path routing algorithms for wireless networks," *J. Parallel Distrib. Comput.*, vol. 63, no. 1, pp. 22–32, 2003.
- [63] D. S. Corp., "iButton HomePage." [Online]. Available: <http://www.ibutton.com>, as viewed July, 2003

REFERENCES

- [64] K. Fall and K. Varadhan, "The NS Manual (Formerly NS Notes and Documentation)," 2002. [Online]. Available: citeseer.ist.psu.edu/article/fall03ns.html
- [65] "The CMU Monarch Project. The CMU Monarch Project's Wireless and Mobility Extensions to NS," 1998. [Online]. Available: citeseer.ist.psu.edu/monarch98cmu.html
- [66] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, vol. 2, no. 5, pp. 483–502, 2002. [Online]. Available: citeseer.ist.psu.edu/camp02survey.html
- [67] I. Stojmenovic, "Position-based routing in ad hoc networks," *IEEE Communications Magazine*, vol. 40, no. 7, pp. 128–134, 2002.
- [68] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.
- [69] J. Kong and X. Hong, "ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in *the 4th ACM international symposium on Mobile ad hoc networking and computing*, pages 291–302. ACM Press, 2003., 2003. [Online]. Available: citeseer.ist.psu.edu/kong03anodr.html
- [70] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*. Springer-Verlag, 2001, pp. 552–565.
- [71] Y. Kim, J. Lee, and A. Helmy, "Impact of location inconsistencies on geographic routing in wireless networks," *ACM Mobile Computer and Communications Review (MC2R), Special issue on Wireless PAN and Sensor Networks*, vol. 8, no. 1, 2004.
- [72] J. Li, C. Blake, D. S. D. Couto, H. I. Lee, and R. Morris, "Capacity of ad hoc wireless networks," in *MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM Press, 2001, pp. 61–69.

REFERENCES

- [73] V. Shoup, "Practical threshold signatures," *Lecture Notes in Computer Science*, vol. 1807, pp. 207–220, 2000. [Online]. Available: cite-seer.nj.nec.com/shoup99practical.html
- [74] R. Ostrovsky and M. Yung, "How to withstand mobile virus attacks," in *Proceedings of the 10th Annual ACM Symposium on Principles of Distributed Computing*, 1991, pp. 51–59.
- [75] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive Secret Sharing Or: How to Cope With Perpetual Leakage," *Lecture Notes in Computer Science*, vol. 963, pp. 339–352, 1995. [Online]. Available: cite-seer.nj.nec.com/herzberg95proactive.html