Study on Anonymous Routing and Untraceable Secure Communications in Wireless Mobile Ad-hoc Networks

March 2007

Sk. Md. Mizanur Rahman

Study on Anonymous Routing and Untraceable Secure Communications in Wireless Mobile Ad-hoc Networks

Graduate School of Systems and Information Engineering

University of Tsukuba

March 2007

Sk. Md. Mizanur Rahman

Abstract

The subject of this dissertation is anonymous routing and secure communications in wireless mobile ad-hoc networks. In such networks packets are relayed over multiple hops to reach their destination. In order to communicate in ad-hoc networks, many routing protocols have been proposed. Concerning nodes location in networks, researchers have divided routing protocols basically in two groups, namely position-based routing and topology-based routing.

Due to the infrastructure-less, dynamic, and broadcast nature of radio transmissions, communications in mobile ad-hoc networks, are susceptible to malicious traffic analysis. After performing traffic analysis, an attacker conducts an intensive attack (i.e., a target-oriented attack) against a target node specified by the traffic analysis. Because of the degradation of both throughput and security of routing, traffic analysis and its subsequent target-oriented attack are known as serious problems in regards to mobile ad-hoc networks. Also malicious intermediate nodes in wireless mobile ad-hoc networks are a threat concerning security as well as anonymity of exchanged information. Thus, to prevent such kinds of attack and to prevent anonymity of nodes in network, anonymous secure communication is necessary.

This dissertation is concerned with the development and evaluation of such protocols, both in position-based and in topology-based routing strategies. Three years before it was an open problem for position-based routing strategy to design an anonymous routing protocol. Basically, position information of routing nodes is very sensitive data in mobile ad-hoc networks, where even nodes not knowing each other establish a network temporarily. It is desirable that position information is kept secret. All of these problems are especially

prominent in position-based routing protocols of mobile ad-hoc networks. Therefore a new position-based routing protocol, Anonymous On-demand Position-based Routing (AODPR), which keeps routing nodes anonymous, thereby preventing possible traffic analysis, is proposed. The proposed scheme uses a time-variant temporary identifier, Temp ID, which is computed from the time and position of a node and used for keeping the node anonymous. Only the position of a destination node is required for the route discovery, and the Temp ID is used for establishing a route for sending data. A receiver dynamic-handshake scheme is designed for determining the next hop on-demand by using the Temp ID. The level of anonymity and the performance of this scheme were evaluated. The evaluation results show that the proposed scheme ensures the anonymity of both route and nodes and robustness against a target-oriented attack and other attacks. Moreover, this scheme does not depend on node density as long as nodes are connected in the network.

To protect anonymity and achieve security in topology-based routing strategy of mobile ad-hoc networks, an anonymous on-demand routing protocol, namely, Routing with Indeterminate Objects for Mobile ad-hoc networks Observer (RIOMO) is proposed. In this protocol pseudo IDs of nodes are generated considering Pairing-based Cryptography. Nodes can generate their own pseudo IDs independently. As a result RIOMO reduces pseudo IDs maintenance costs. Only trust-worthy nodes are allowed to take part in routing to discover a route. To ensure trustiness each node has to make authentication to its neighbors through an anonymous authentication process. Thus RIOMO safely communicates between nodes without disclosing node identities; it also provides different desirable anonymous properties such as identity privacy, location privacy, route anonymity, and robustness against several attacks.

Acknowledgements

I am ever grateful to my advisor esteemed Professor Eiji Okamoto for his imperturbable advice, enduring support, and continual help throughout my time in the non degree research program as well as in the Ph.D. program. I also appreciate very much the fact that he took me seriously when I communicated with him four years ago asking about the possibility of taking me as a Ph.D. student in his laboratory "Cryptography and Information Security" in the Graduate School of Systems and Information Engineering, University of Tsukuba. His kind words at that time gave me the necessary encouragement to proceed and come to the University of Tsukuba, Tsukuba, Japan. I earnestly thank my adviser for his excellent comments and guideline during my research period in the University of Tsukuba. The immense trust he imposed in my abilities was always a great source of motivation.

Special thanks go to my co-advisor, Atsuo Inomata, who is most responsible for helping me challenging research that lies behind this dissertation. Dr. Inomata became a friend and mentor within this period. He taught me how to work hard, made me a better programmer, had confidence in me when I doubted myself, and brought out the good ideas in me. Without his encouragement and constant guidance, I could not have finished this dissertation. In his work schedule he always came to my desk to talk about my ideas and to ask me intellectual questions to help me think through my problems. He supported me to overcome any kind of problems whether it is philosophical, analytical, and computational or even it is personal.

Very special thanks go to my co-advisor Associate Professor Masahiro Mambo, who is most responsible for helping me complete the writing of this dissertation. He taught me how to write academic papers and prepare research presentation slides. He regularly met me at my desk to discuss various interesting

questions about my ideas, to proofread and mark up my papers and chapters, and to ask me intellectual questions to help me through my problems. Without his guideline and teaching it would have been impossible to finish this dissertation. I am grateful to him for giving me enough time and encourage to consider a problem with different aspect and to find a better solution.

Thanks go to Assistant Professor Takeshi Okamoto as my co-advisor, who is most responsible for managing everything in the laboratory and to maintain a peaceful and friendly environment for research. He was always generous to me and to overlook my little mistakes. His intellectual comments about my research presentation encourage me to prepare fruitful presentation slides, thus I overcame all of my previous presentation sessions.

Besides my advisors, I would like to thank all committee members for their comments and advice during the preliminary examinations. Special thanks to Professor Yuko Murayama, Professor Kazuhiko Kato, Associate Professor Jie Li, for the discussion and advice on several topics and insightful comments.

This dissertation would not have been possible without the financial support I received from the Japan Government Ministry of Education, Culture, Sports, Science and Technology (MEXT); as a Monbukagakusho University Recommended Fellowship student, recommended by Professor Eiji Okamoto.

I would also like to say "thank you" to the following people at the Laboratory of Cryptography and Information Security to have confidence in me and for supporting my research. Jean-Luc Beuchat (Researcher), for helping me to review my preliminary examinations presentation slides as well as to check proofread some of my writings, Naoki Kanayama (Researcher), for mental support in different situations, Raylin Tso (Researcher), for helping at any time about the traveling information for attending conference, Tadahiko Itoh (Doctoral Program), for helping to manage residence as well as to discuss about Japanese lifestyle when I was new to Japan, Fumiaki Kanazawa (Doctoral Program), for helping me when I faced different difficulties in everyday life. Hiromi Yamaguchi, Keiko Ueki, Misae Kobayashi and Asumi Watanabe for their

continuous support for different office works as well as for helping desk works. Several other people those who have been helpful directly or indirectly and others I might have missed.

I am also very much grateful to many teachers in the past: Professor Dr. Chowdhury Mofizur Rahman (Pro-Vice Chancellor & Head, CSE Dept., United International University (UIU), Dhaka; Ex-head, Department of Computer Science & Engineering, Bangladesh University of Engineering & Technology (BUET)), for getting me interested in artificial intelligence and Prolog programming, Professor Dr. M. Lutfar Rahman (Department of Computer Science and Engineering, University of Dhaka), for getting me interested in security protocols and applications, Dr. Shahida Rafique (Professor & Ex-chairman, Department of Applied Physics, Electronics & Communication Engineering, University of Dhaka), for getting me interested in system analysis and design methodologies, Professor Dr. Qamrun Nessa Begum (Ex-director, Institute of Science & Technology, Dhanmondi, Dhaka), for guiding as parents during my undergraduate level study, Dr. Md. Haider Ali (Chairman, Dept. of Computer Science and Engineering, University of Dhaka), for sharing his experience with me of his study period in Japan also encouraged and helped me to submit application form for Monbukagakusho scholarship. Thanks go to all of my friends of school, college and university level for their encouragements and mental supports.

Last but not least, I thank my family: the departed souls of my parents, Late Md. Mosad Ali Sk, and Late Begum Rezia Khatun, for giving me life in the first place, for encouraging me for whole of my educational life. Thanks go in order according to the eldest of my brothers and sisters; S. M. Elias Ali to support my secondary and higher secondary school level study, S. M. Mahfuz Alam, S.M. Mahboob Alam, S. M. Muzahid Alam for their continuous mental support and encourage towards Ph.D. level study. Special thanks go to my immediate second elder and immediate elder brothers Sk. Md. Motiar Rahman and Sk. Md. Atiar Rahman for their time and maintaining daily life requirements during my

Graduate and Masters level studies. Also thanks goes to my sisters Begum Rawson Ara Khatun and Nasim Ara Khatun for their encouragements and mental support.

Special thanks go to my wife, Tania Islam for her continuous hard work to maintain daily life in Tsukuba, also mental supports and encouragements to avoid frustration during my critical busy time and mental pressure. She also discussed with me about the result of my research to notify me that it should always be useful and provide good ambition for mankind.

© Copyright by
Sk. Md. Mizanur Rahman
March 2007

Department of Risk Engineering
(Cyber Risk)

Dissertation submitted in accordance with the requirements for the degree
Doctor of Philosophy in Engineering

Graduate School of Systems and Information Engineering

University of Tsukuba, Japan

March 2007

Dedicated to the departed souls of my parents who have made this possible and also to all the people who have helped or heartened me

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND ABBREVIATIONS

ACK- Acknowledgment

ANODR- Anonymous on-demand routing

AO2P-Ad hoc on-demand position-based private routing

AODV- Ad hoc on-demand distance vector

AODPR-Anonymous on-demand position-based routing

AP- Access point

ARAN- Secure routing protocol for ad-hoc networks

CSMA/CA- Carrier sense multiple access with collision avoidance

CTS- Clear to send

DIFS- Distributed inter frame space

DISPOSER- Distributed secure position service

DL- Discrete logarithm

DSDV- Destination sequenced distance vector

DSR- Dynamic source routing protocol

GPS- Global positioning system

IBSS- Independent basic service set

IETF- Internet engineering task force

LAR- Location-aided routing

LPI/LPD- Low probability of interception/Low probability of detection

MANET- Mobile ad hoc network

MD5- Message digest algorithm 5

OLSR- Optimized link state routing

OSPF- Open shortest path forwarding

RF- Radio frequency

RFC- Request for comments

RIOMO- Routing with indeterminate objects for mobile ad-hoc networks observer

RTS- Request to send

SDDR-Secure dynamic distributed topology-based routing

SEAD- Secure efficient distance vector routing for mobile wireless ad hoc networks

SHA-1-Secure hash algorithm 1

SIFS- Short inter frame space

SRP- Secure routing protocol

SUCV- Secured with statistically unique and cryptographically verifiable

TBRPF-Topology broadcast based on reverse-path forwarding

VHR- Virtual home region

CHAPTER 1

INTRODUCTION

A mobile ad-hoc network is a collection of two or more devices equipped with wireless communications and networking capability. Such devices can communicate with another node that is within their radio range or one that is used to relay or forward the packet from the source toward the destination. Ad-hoc networks are intranets and they remain as intranets unless there is connectivity to the Internet. Such confined communications have already isolated attackers who are not local in the area.

Conventional wireless mobile communications are normally supported by a fixed wire/wireless infrastructure. A mobile device would use a single-hop wireless radio communication to access a fixed base-station that connect it to the wire/wireless infrastructure. In contrast, ad-hoc networks do not use any fixed infrastructure, it is a self-configuring network of mobile stations connected by wireless links and defined as IBSS in IEEE 802.11 standards. The nodes in a mobile ad-hoc network intercommunicate via single-hop and multi-hop paths in a peer-to-peer fashion without using AP. Intermediate nodes between a pair of communicating nodes act as routers [1]. Thus the nodes operate both as hosts and routers. The nodes in the ad-hoc network could be potentially mobile, and so the creation of routing paths is affected by the addition and deletion of nodes. The topology of the network may change randomly, rapidly, and unexpectedly [1]. Neighbors are friendly or hostile, information sent in an ad-hoc route can be protected in some way but since multiple nodes are involved, the relaying of packets has to be authenticated by recognizing the originator of the packet and the flow ID or label.

The concept of mobile ad-hoc networking opens a broad spectrum of potential applications in both military and civilian systems owing to their self-configuration and self maintenance capabilities. The first, and the most important scenario, is the ability to establish a network in places where it's not possible otherwise: i.e., in a disaster relief setting, or in a situation where the entire communication structure has been destroyed. Collaborative computing and communications in smaller areas (building organizations, conference, etc.) can setup using ad-hoc networking technologies [1]. The use of these networks has increased dramatically, and they're being used for implementing solutions for business, entertainment, and safety applications in business, residential, and industrial areas. Communications in battlefields are other example of application environments. Many of these applications, such as military battlefield operations, homeland-security scenarios, law enforcement, and rescue missions are security sensitive. As a result, security in mobile ad-hoc networks, MANETs, has recently been drawing much attention [2].

Traffic analysis is one of the most subtle and unsolved security attacks against MANETs. By definition, it is an attack such that an adversary observes network traffic and infers sensitive information of the applications and/or the underlying system [3]. Sensitive information includes the identities of communicating parties, network traffic patterns [2], and their changes. The leakage of such information is often devastating in security-sensitive scenarios. For example, an unexpected change of the traffic pattern in a military network may indicate a forthcoming action, a chain of commands, or a state change of network alertness [4]. It may also reveal the locations of command centers or mobile VIP nodes, which will enable the adversaries to launch pinpoint attacks on them. In contrast to active attacks, which usually involve the launch of denial of service or other more “visible” and aggressive attacks on the target network, traffic analysis is a kind of passive attack, which is “invisible” and

difficult to detect. It is therefore important to design countermeasures against such malicious traffic analysis.

The shared wireless medium of MANETs introduces opportunities for passive eavesdropping on data communications. Adversaries can easily overhear all messages “flying in the air” without physically compromising nodes. Several methods for withstanding eavesdropping and other kinds of traffic analysis have been investigated. One attempt is to prevent the wireless signals from being intercepted or even detected by developing LPI/LPD (low probability of interception/low probability of detection) communication techniques. Examples of such techniques include spread-spectrum modulation, effective power control, and directional antennas [5]. However, it is impossible to completely avoid signal detection in open wireless environments. The second method relies on the use of traffic padding, i.e., inserting dummy packets into the network [6] to camouflage the real traffic pattern. However, this approach adds significant extra load to the network and consumes scarce network resources. The third method is to perform end-to-end encryption and/or link encryption on data traffic. However, this only prevents adversaries from accessing traffic contents. Adversaries can still carry out traffic analysis based on the bare network-layer and/or MAC addresses, both of which are unprotected and unencrypted in common ad-hoc routing protocols such as Ad hoc On-Demand Distance Vector (AODV) [7]. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) [8], and the de facto MAC protocol IEEE 802.11.

Research on ad-hoc networks has resulted in a number of routing protocols suitable for MANETs [9]. Most current researches on MANET routing are focused on *topology-based* protocols. These protocols use information about links in the network to perform packet forwarding and are generally classified as either table-driven or on-demand. The on-demand

scheme is more familiar than the table-driven one because it does not involve extra computation like routing table maintenance of the table-driven scheme.

Meanwhile *position-based* routing protocols are known to be a good alternative to on-demand topology-based protocols in many cases [10, 11]. *Position-based* routing protocols use a node's geographical position to make routing decisions, resulting in improved efficiency and performance. Therefore, nodes of these protocols are required to obtain their own geographical position and the geographical position of the destination. Generally, this information is obtained via global positioning system (GPS) and location services.

Most traditional *topology-based* MANET protocols were designed with reliability and performance in mind. Unfortunately these protocols were not designed to be secure and do not defend against malicious attacks. AODV and DSR, two protocols under consideration for standardization by the IETF MANET Working Group, are both vulnerable to a number of attacks, including impersonation, modification, and fabrication [12]. *Position-based* MANET routing protocols [10, 13, 14] are also vulnerable to such attacks, as they focus on improving performance while disregarding security issues. In addition, these protocols lack cryptographic techniques to protect location information exchanged between nodes, revealing the exact location of nodes to anyone within range. In a high-risk environment, this is unacceptable. Cryptographic techniques must be employed to protect position information in these protocols if they are to be used in a high-risk MANET.

1.1 Motivation

In fixed networks, routing does not affect network topology which is physically determined a priori. However, this is not true in mobile ad-hoc networks where network topology constantly changes due to mobility. Once

information about the network topology is revealed, the adversary can break the network's anonymity protection given other out of-band information like geographic positions and physical boundaries of the underlying mobile network; also adversaries can setup attacks such as active attack, passive attack including target oriented attack, some other attacks namely wormhole attack, timing attack, rushing attacks, etc. So, privacy of network topology becomes a new anonymity aspect in mobile ad-hoc networks. Thus anonymity is one of the most important factors for securing ad-hoc network communications, where the intruders do not know about the communication IDs. It ensures that a user may use a resource or service without disclosing the user's identity. The requirements for anonymity provide protection of the user identity. Anonymity requires that other users or subjects are unable to determine the identity of a user bound to a subject or operation [15]. If less is known about the linking to a subject, then Anonymity is the stronger. As a result, adversaries fail to make correlation between the eavesdropped traffic information and the actual network traffic patterns. Thus traffic analysis attack can be efficiently defeated. The strength of anonymity decreases with increasing knowledge of the pseudonym linking. To keep the strength of anonymity strong, it should be considered in designing anonymous protocol that intruders can not increase their knowledge about pseudonym linking.

1.2 Contributions and Organization of the Dissertation

Since nodes in MANETs move dynamically, adversaries cannot conduct active attacks without knowing the location or name of nodes. It thus often happens that traffic analysis is conducted passively at first and active attacks are conducted later. Therefore, we set our goal to establish protocols for both

in *position-based* scheme as well as in *topology-based* scheme that are secure against passive attacks in terms of the privacy notions explained in chapter 2 and also secure against the several active attacks.

To the best of our knowledge when we started our research it was an open problem for *position-based* routing strategy to design an anonymous routing protocol. But, at the end of our proposed protocol there is also an available anonymous protocol, Ad hoc on-demand position-based private routing (AO2P) [16], which does not ensure location privacy properly. To achieve communication anonymity and security in any node density network, we propose a new position-based anonymous routing protocol, called an anonymous on-demand position-based routing (AODPR), which keeps routing nodes anonymous. In AODPR, the position of the destination is encrypted with a common key of nodes, and this encrypted position is used for the routing. Information is thus not disclosed to nodes not composing the ad-hoc network. In AODPR, a route is discovered by a dynamic handshake mechanism, which dynamically determines the next hop. For this purpose, a route-request message is sent from the source towards the position of the destination.

There are some recent *topology-based* proposals [17, 18, 19, 20, 21, 22] which will be discussed on chapter 3, taking care of privacy in MANETs. Among the existing protocols, one protocol can not provide all the security and anonymous properties in terms of security notions of chapter 2. In MASK [22] system administrator generates a large number of pseudo IDs set for each node in the network. To keep anonymity in MASK, every node should have to manage a huge umber of pseudo IDs provided by the system administrator, which is costly for ad-hoc network communication in terms of extra task for nodes, namely IDs maintenance cost. So, to avoid extra pseudo IDs maintenance cost and to achieve strong communication anonymity and security, an anonymous on-demand routing protocol called Routing with

Indeterminate Objects for Mobile ad-hoc networks Observer (RIOMO), is proposed. In RIOMO, every node can generate its own pseudo IDs dynamically only from one pseudo ID taken form the system administrator. Thus pseudo IDs maintenance cost is reduced compared to MASK by Zhang et al., [22]. The comparison results are discussed in chapter 3.

Organization of the Dissertation

This dissertation consists of seven chapters. In Chapter 1, introduction of ad-hoc mobile networks with its application is described, also security aspects is discussed. In the same chapter motivation and contributions of this research are discussed. Finally outline of this dissertation is given in this chapter. In Chapter 2, security notions and preliminaries of wireless property of ad-hoc network are given first and cryptographic security properties are also discussed. Some related mathematic background, including bilinear pairings and computational problems is provided. Chapter 3 is a place for the discussion of our result and the comparison analysis with the existing anonymous protocols are given, also result is discussed. Chapter 4 and 5, are considered as the principle contributions of this dissertation. In Chapter 4, proposed new algorithm for *position-based* routing strategy is described; in section 4.1 AODPR fundamentals are defined also an assumption is discussed. In section 4.2 parameters and overview is discussed in terms of nodes functionalities. Section 4.3 is dedicated for the AODPR operation procedures. Section 4.4 investigates the anonymity and security properties of the proposed protocol. Chapter 5 is another contribution in *topology-based* anonymous routing, based on pairing-based crypto properties; here proposed protocol RIOMO is discussed. In Section 5.1 architecture and design of the protocol is described. In Section 5.2 anonymous neighbor authentication process is clearly defined. Section 5.3 and 5.4 are dedicated for the control packets and

routing procedures for RIOMO. In Chapter 6 performance analysis is discussed; in section 6.1 theoretical analysis of AODPR, and section 6.2 is the simulation result of the same protocol. The security analyses of these schemes are also investigated in this chapter. Finally, in Chapter 7 conclusion with future works and open problems are discussed.

1.3 Publications and Origins of Contributions

This dissertation contains research published with my advisor Professor Dr. Eiji Okamoto, co-advisors Researcher Dr. Atsuo Inomata, Associate Professor Dr. Masahoro Mambo and Assistant Professor Dr. Takeshi Okamoto. Some contents of Chapter 4, AODPR anonymous routing protocol for *position-based* scheme, first appeared in [C2] and was later improved on and published in [J1]. The RIOMO anonymous routing protocol for *topology-based* scheme of Chapter 5 was originally described in [C1] and [S1]. Concepts, related to hash function and symmetric encryption was taken form my previous research published in [J2, J3, J4, J5, C6, C7, C8, and C11].

CHAPTER 2

PRELIMINARIES

Privacy and security notions and preliminaries of wireless property of ad-hoc network are discussed in this chapter. Cryptographic security properties with some related mathematical background, including bilinear pairings and computational problems are provided in this chapter.

2.1 Privacy and Security Notions

The key notions on privacy associated with MANETs are summarized as follows.

Identity Privacy: Identity privacy means no one knows the real identity of the nodes in the network. We are especially interested in discussing identity privacy of entities involved in packet transmission, namely, the source, intermediate nodes and the destination.

Location Privacy: Requirements for location privacy are as follows: (a) no one knows the exact location of a source or a destination, except themselves; (b) other nodes, typically intermediate nodes in the route, have no information about their distance, i.e., the number of hops, from either the source or the destination. It is said that a protocol satisfying (a) achieves weak location privacy and a protocol satisfying both (a) and (b) achieves strong location privacy.

Route Anonymity: Requirements for route anonymity are as follows: (a) adversaries either in the route or out of the route cannot trace packet flow back

to its source or destination; (b) adversaries not in the route have no information on any part of the route; (c) it is difficult for adversaries to infer the transmission pattern and motion pattern of the source or the destination.

Passive Attacks: Passive attack typically involves unauthorized "listening" to the routing packets or silently refusing execution of the function requested. This type of attack might be an attempt to gain routing information from which the attacker could extrapolate data about the positions of each node in relation to the others. Such an attack is usually impossible to detect, since the attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routed traffic.

Active Attacks: Active attacks are meant to degrade or prevent message flow between nodes. They can cause degradation or a complete halt in communications between nodes. Normally, such attacks involve actions performed by adversaries, e.g., replication, modification, and deletion of exchanged data.

DoS: DoS attacks occur when an attacker overloads nodes with useless traffic so that legitimate requests cannot be processed and resources cannot be accessed. The packets sent to the target will have randomly selected return addresses and often spoofed source addresses, so the target has difficulty finding the exact location of the attack

Multiple adversaries such as I_1, I_2, I_3, and I_4 in co-operation can set a specific node N, as a target in order to exhaust the resource of that node, as in Figure 2.1. One adversary I, with enough power, as in fig. 2.2., can set specific nodes N_1, N_2, N_3, N_4 as target in order to exhaust the resource of the nodes. Main concept is to identify node and make a target to the specific node.

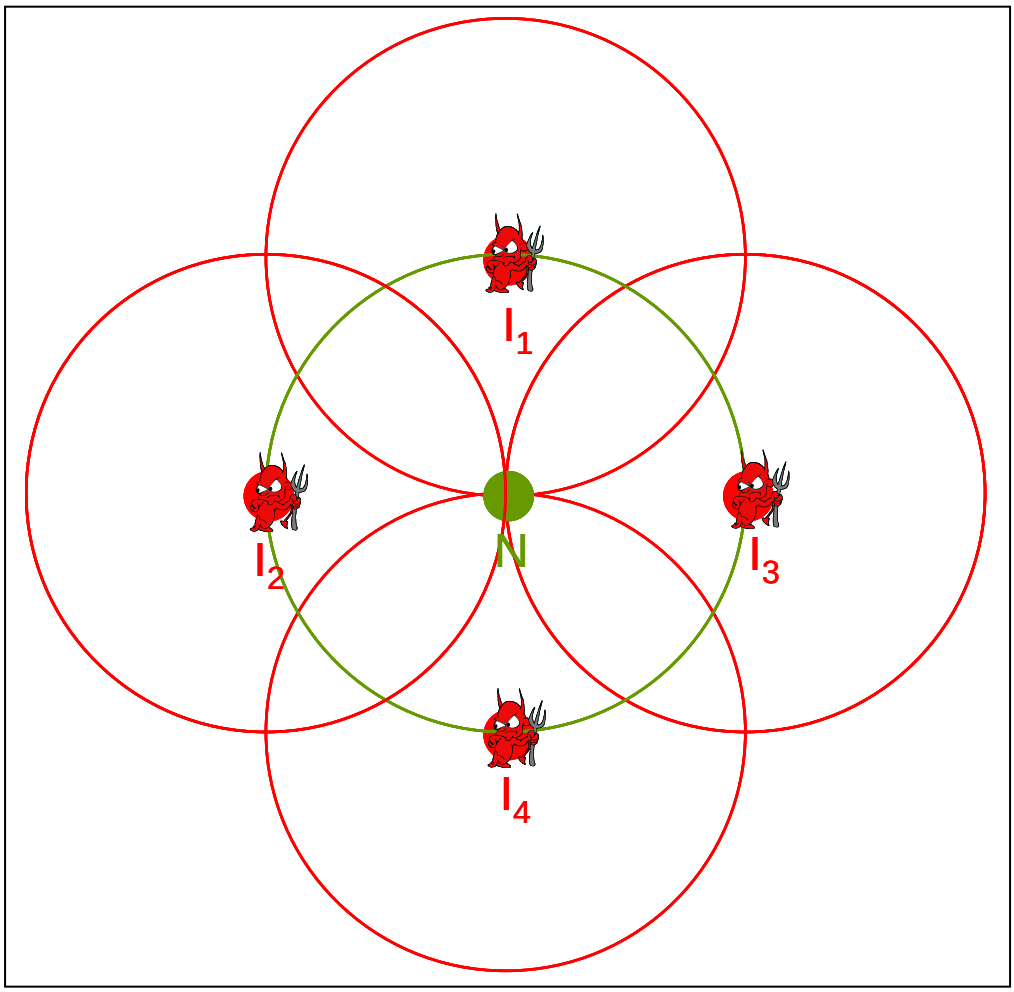

Figure 2.1: DoS, according to the target; Multiple-to-One

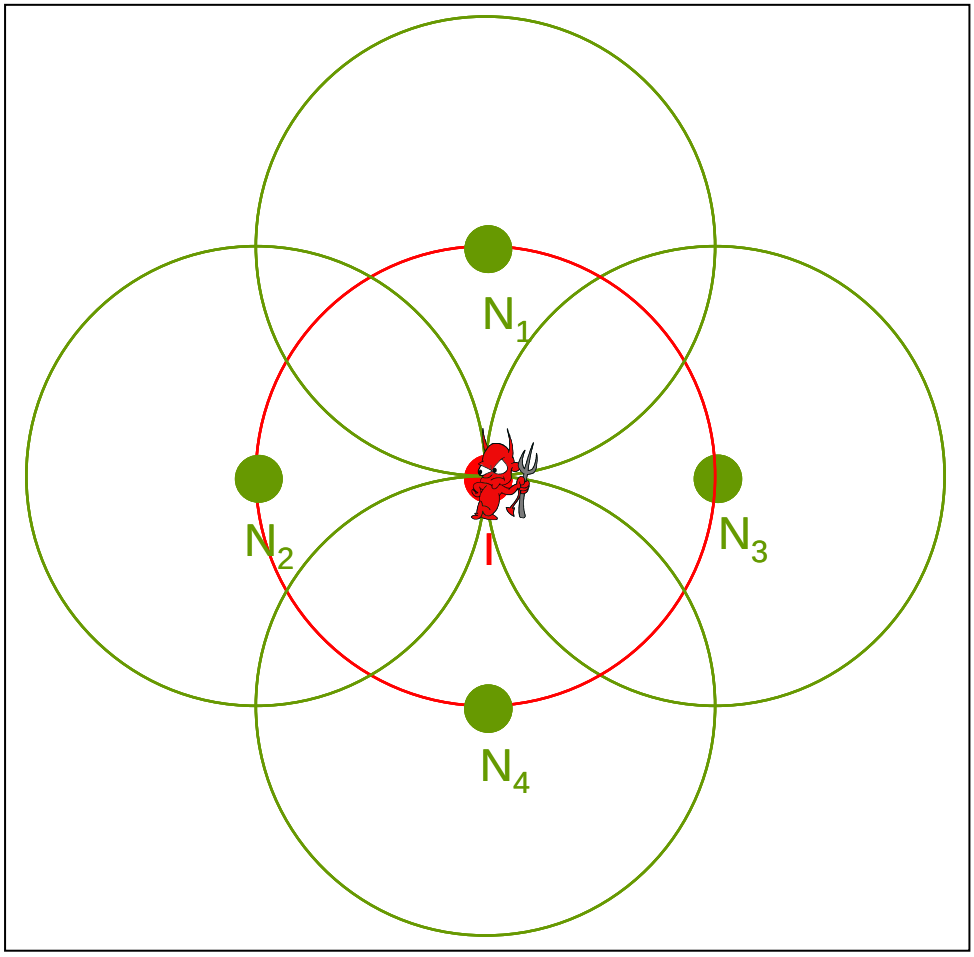

Figure 2.2: DoS, according to the target; One-to-Multiple

Wormhole Attacks: In wormhole attack, an attacker records a packet in one location of the network and sends it to another location through a high quality out-of-band link namely tunnel [23] made between the attacker's nodes in the network. Figure 2.3 shows a basic wormhole attack. The attacker replays packets received by I_1 at node I_2, and vice versa. If it would normally take several hops for a packet to traverse from a location near I_1 to a location near I_2, packets transmitted near I_1 traveling through the wormhole will arrive at I_2 before packets traveling through multiple hops in the network. The attacker can make S and D believe they are neighbors by forwarding routing

messages, and then selectively drop data messages to disrupt communications between S and D. For most routing protocols, the attack has impact on nodes beyond the wormhole endpoints' neighborhoods also. Node S will advertise a one-hop path to D so that C will direct packets towards D through S. For example, in on-demand routing protocols (DSR [8] and AODV [7]) or secure on-demand routing protocols (SEAD [26], Ariadne [39], SRP [43]), the wormhole attack can be mounted by tunneling ROUTE REQUEST messages directly to nodes near the destination node. Since the ROUTE REQUEST message is tunneled through high quality channel, it arrives earlier than other requests. According to the protocol, other ROUTE REQUEST messages received for the same route discovery will be discarded. This attack thus prevents any other routes from being discovered, and the wormhole will have full control of the route. The attacker can discard all messages to create a denial-of-service attack, or more subtly, selectively discard certain messages to alter the function of the network [27]. An attacker with a suitable wormhole can easily create a sinkhole that attracts (but does not forward) packets to many destinations. An intelligent attacker may be able to selectively forward messages to enable other attacks and also be able to place wormhole endpoints at particular locations. Strategically placed wormhole endpoints can disrupt nearly all communications to or from a certain node and all other nodes in the network [27].

The neighbor discovery mechanisms of periodic (proactive) routing protocols such as DSDV [28], OLSR [29], and TBRPF [30] rely heavily on the reception of broadcast packets as a means for neighbor detection, and are also extremely vulnerable to this attack.

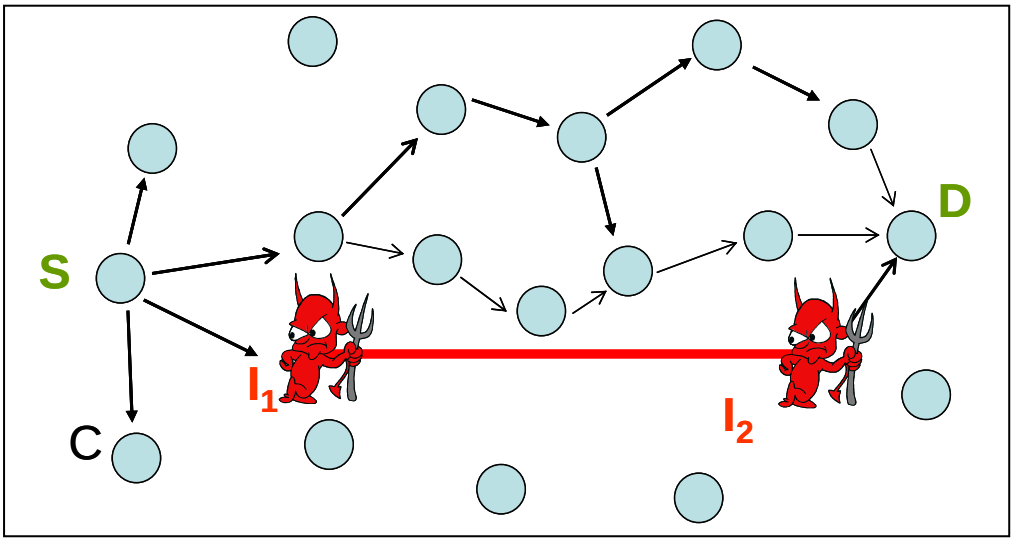

Figure 2.3: Wormhole attack: The adversary controls nodes I_1 and I_2 and connects them through a low-latency link.

Rushing Attack: Existing on-demand routing protocols forward a request packet that arrives first in each route-discovery. In the rushing attack, the attacker exploits this property of route discovery operation as shown in Figure 2.4. The initiator node initiates a Route Discovery for the target node. If the ROUTE REQUESTs for this Discovery forwarded by the attacker are the first to reach each neighbor of the target (shown in gray in the figure), then any route discovered by this Route Discovery will includes a hop through the attacker [52]. That is, when a neighbor of the target receives the rushed REQUEST from the attacker, it forwards that REQUEST, and will not forward any further REQUESTs from this Route Discovery. When non-attacking REQUESTs arrive later at these nodes, they will discard those legitimate REQUESTs. As a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes).

In general an, attacker can forward a route request more quickly than legitimate nodes can, so it can enter in a route. Such a route can not be easily detected.

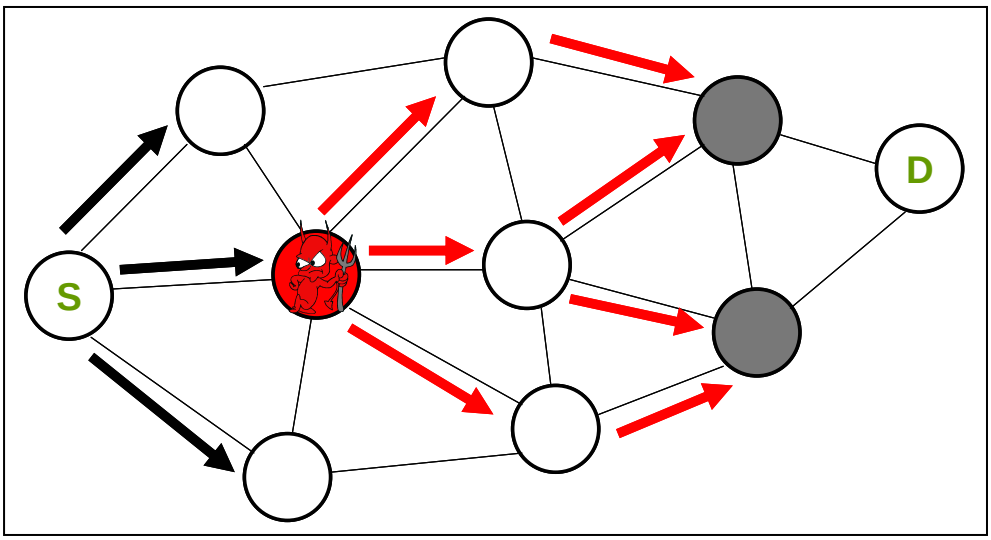

Figure 2.4: Network illustrating the rushing attack

2.2 Characteristics of Wireless Communication System

One of the major challenges in ad hoc networks security is that ad hoc networks typically lack of a fixed infrastructure both in form of physical infrastructure such as routers, servers and stable communication links and in the form of an organizational or administrative infrastructure [24]. Another difficulty lies in the highly dynamic nature of ad hoc networks since new nodes can join and leave the network at any time. The major problem in providing security services in such infrastructure-less networks lies on how to manage the cryptographic keys that are needed. When designing protocols for ad hoc networks, whether routing protocols or security protocols, it is

important to consider the characteristics of the network and realize that there are many "flavours" of ad hoc networks. Ad-hoc wireless networks generally have the following characteristics [25]:

Dynamic network topology: The network nodes are mobile and thus the topology of the network may change frequently. Nodes may move around within the network, the network can be partitioned into multiple smaller networks or be merged with other networks.

Limited bandwidth: The use of wireless communication typically implies a lower bandwidth than that of traditional networks. This may limit the number and size of messages sent during protocol execution.

Energy constrained nodes: Nodes in ad hoc networks will most often rely on batteries as their power source. The use of computationally complex algorithms may not be possible. This also exposes the nodes to a new type of denial of service attack, the sleep deprivation torture attack [25] that aims at depleting the nodes energy source.

Limited physical security: The use of wireless communication and the exposure of the network nodes increase the possibility of attacks against the network. Due to the mobility of the nodes the risk of them being physically compromised by theft, loss or other means will probably be greater than that for traditional network nodes. In many cases the nodes of ad hoc network may also have limited CPU performance and memory, e.g. low-end devices such as PDA's, cellular phones and embedded devices. As a result certain algorithms that are computationally or memory expensive might not be applicable.

2.3 Bilinear Maps

The anonymous authentication procedure that we propose in our RIOMO protocol is based on the Bilinear Pairings. The bilinear pairing such as Weil

pairing or Tate Pairing on elliptic and hyper elliptic curves has recently been found applications in design of cryptographic protocols.

Elliptic Curves

$E(F_q) : y^2 = x^3+Ax+B$, Elliptic curves are considered interesting primarily as an alternative group structure, with certain advantages when it comes to the implementation of common cryptographic protocols. The main advantage is that much smaller keys can be used, as there is no known polynomial-time algorithm for the discrete logarithm problem for the great majority of such curves. Given a point *P* on a curve *E* defined over a finite field F_q where $q = p^m$, and p is a large prime; this is the problem of determining '*a*' for given '*aP*'. In most circumstances the points on such a curve form a simple cyclic group. Each point on the curve has an order. This is the smallest positive integer *r* such that $rP = O$, where *O* is the identity point of the group, the so-called point at infinity. The number of points on the curve, the order of the curve, is referred to as *#E*. Every valid *r* divides *#E*. We also need to know the important relationship $\#E = q+1-t$, where *t* is the *trace of the Frobenius*, and *t* is relatively small - a constant for each curve. We note also the "twisted" curve, $E^t(Fq) : y^2 = x^3+ d^2Ax+ d^3B$, where *d* is any Quadratic Non Residue mod *q*. This curve has $\#E^t = q+1+t$ points on it [53].

The Embedding Degree

However something rather magical happens when a curve with the same equation is considered over the field F_{q^k} for a certain value of *k*. The group structure undergoes a strange blossoming, and takes on a new, more exotic character. The smallest value of *k* for which this happens is referred to as the *embedding degree*. For a random curve the embedding degree will be very

large. However it can be as small as k=1, and it is not in fact difficult to find curves for any positive value of k. Here for simplicity we concentrate on the particular case k=2 and q=p a prime. In the field F_{p^2} (called the *quadratic extension* field) elements are represented as (a,b) which is $a+ib$ where i is the "square root" of a QNR. If p = 3 mod 4 one can conveniently choose the QNR as $p-1$.

A k=2 curve $E(Fp)$ has $p+1-t$ points on it. Lets this set of points is S. It contains a subgroup of points of prime order r and a representative of these is a point P. The same curve over $E(F_p^2)$ will have $\#E(F_p^2) = (p+1-t)(p+1+t)$ points on it, as a consequence of Weil's Theorem. For a k=2 curve r exactly divides $p+1$ and ($p+1-t$), and hence necessarily r divides t. And r^2 divides $\#E$.

An example will be useful. The curve is $E(F_{131}) : y^2 = x^3-3x+8$, with p =131, r =11, t=22, P(123,100), #E=110. There are points on the curve of order 110, and the group is cyclic. There is a subgroup of order r. The curve is not supersingular. The twisted curve is $E^t(F_{131}) : y^2 = x^3-3x-8$, And $\#E^t$ = 154. This same curve taken over the extension field $E(F_p^2)$ has 16940=154.110 points on it. And there are no points on the curve of this order, it is not cyclic. Here a point on this curve is represented as $Q[x,y] = Q[(a,b),(c,d)]$

Group Structure

There are a couple of ways of considering all these points. But at first some notation will be discussed. The complete set of curve points is called G, of order $\#E$. The set of all points that are transformed to O by multiplication by r ("killed by r") is called $G[r]$. These are the r-torsion points. Since r is prime, this is all the points of order r plus O. There are r^2 such points, and these r^2 points can be organized as $r+1$ distinct cyclic subgroups of order r - they all share O. Note that one of these subgroups is $S[r]$ and consists of all those r-

torsion points from the original curve $E(F_p)$, points of the form $Q[(a,0),(c,0)]$, which are of course on both curves.

Let $h = \#E/r^2$. Then a random point on the curve can be mapped to a point in one of these sub-groups of order r by multiplying it by this co-factor h. For simplicity we assume that r does not divide h. For example curve r=11 and h=140. The set of distinct points generated by multiplying every element of G by r is called rG. The number of elements in rG is h. This is called a *coset*.

Consider the partitioning of the $\#E$ points into distinct *cosets*. This can be done by adding a random point R to every element of rG. There are exactly r^2 such distinct cosets, each with h elements.

The original coset rG is the unique coset that contains O. Every coset contains exactly one r-torsion point. Elements of these cosets are not all of the same order. They do not form a group. The quotient group G/rG is the group formed of all these cosets.

Bilinear pairings

Let G_1 be an additive group and G_2 be a multiplicative group of the same prime order q. Let P be an arbitrary generator of G_1. (*aP denotes P added to itself a times*). Assume that discrete logarithm (DL) problem is hard in both G_1 and G_2. We can think G_1 as a group of points on an elliptic curve over F_q, and G_2 as a subgroup of the multiplicative group of a finite field F_{q^k} for some $k \in Z_q^*$. A mapping $\tilde{e}: G_1 \times G_1 \rightarrow G_2$, satisfying the following properties is called a cryptographic bilinear map.

- *Bilinearity:* $\tilde{e}(aP, bQ) = \tilde{e}(P,Q)^{ab}$ for all $P,Q \in G_1$ and $a, b \in Z_q^*$. This can be restated in the following way. For $P, Q, R \in G_1$, $\tilde{e}(P+Q, R) = \tilde{e}(P,R)\,\tilde{e}(Q,R)$ and $\tilde{e}(P, Q+R) = \tilde{e}(P,Q)\,\tilde{e}(P,R)$.

- *Non-degeneracy:* If P is a generator of G_1, then $\tilde{e}(P,P)$ is a generator of G_2. In other words, $\tilde{e}(P,P)\neq 1$.
- *Computable:* A mapping is efficiently computable if $\tilde{e}(P,P)$ can be computed in polynomial-time for all $P, Q \in G_1$.

Modified Weil Pairing [31] and Tate Pairing [32], [33] are examples of cryptographic bilinear maps.

The Tate Pairing

The Tate Pairing operates on a pair of points, P of prime order r (a member of $G[r]$) and a point Q which is a representative member of one of the cosets, as we already discussed in group structure section, it is denoted as $e_r(P,Q)$. It evaluates as an element of the finite field F_p^2 of order r, observe that r divides p^2-1. Its value is the same irrespective of which element of a particular coset is chosen. Recall that each coset has exactly one r-torsion point. For convenience P is chosen to be a member of $S[r]$, as it also lies on $E(F_p)$, this makes the Tate Pairing calculation much faster [53].

However the Tate pairing can evaluate as 1. This will occur if P is a multiple of Q, which will be the case if Q is chosen from a coset whose r-torsion point is also a member of $S[r]$. For a randomly chosen Q and for large r this is extremely unlikely, the odds are $1/r$.

The Tate Pairing is *non-degenerate* as for any given P not equal to O, we can always find a Q such that $e_r(P,Q)$ is not 1. Also $e_r(P,P)=1$ for P in $S[r]$ (and $k > 1$). However probably the most important property of the Tate pairing is bilinearity $e_r(aP,bQ) = e_r(P,Q)^{ab}$, Note that P must be of order r, but Q need not be.

Which coset to choose Q from? There are computational advantages in choosing points of the form $Q[(a,0),(0,d)]$. Call the set of points of this form T. It is not difficult to see that if there are $p+1-t$ points of the form $Q[(a,0),(c,0)]$

then there will be $p+1+t$ points of the form $Q[(a,0),(0,d)]$. Substitute all $a<p$ for x in the curve equation. Then if the RHS is a QR the point is $Q[(a,0),(\pm c,0)]$, otherwise its $Q[(a,0),(0,\pm d)]$. There will always be a subgroup of order r, consisting of points of this form. Q can therefore be chosen as an element of T. Note that points of this form stay in this form under point multiplication, so such a Q will be in a coset supported by an element of $T[r]$. There are also $p+1+t$ points on the twisted curve. So, Is there a connection between the group of points of the form $Q[(a,0),(0,d)]$ and the group of points on the "twisted" curve? Yes there is - they are *isomorphic*. For every point of the form $Q[(a,0),(0,d)]$ on the curve defined over the quadratic extension field F_p2, there is a point $Q(-a,d)$ on the twisted curve defined over F_p. This is convenient as it means that multiplication of such points can be done on the twisted curve using regular $E(F_p)$ methods.

Operation on Elliptic Curve

Addition of two points on an elliptic curve is defined according to a set of simple rules (e.g., point P_1 plus P_2 is equal to P_4 in Figure 2.5). The addition operation in an elliptic curve is the counterpart to modular multiplication in common public-key cryptosystems, and multiple additions are the counterpart to modular exponentiation. Details of the operations are described as follows.

Elliptic Addition: A straight line running through points P and Q has a third intersection point with the elliptic curve. Point R, namely, the opposite of the third intersection point in relation to the x- axis, as shown in Figure 6, is equivalent to the addition of points P and Q. Thus $P + Q = R$.

Elliptic Doubling: The Tangent line at point P intersects with a different point on the elliptic curve as shown in Figure 2.6. Point R, namely, the opposite point to that intersection point in relation to the x-axis, is equivalent to two times point P. Thus $P+P = [2]*P = R$.

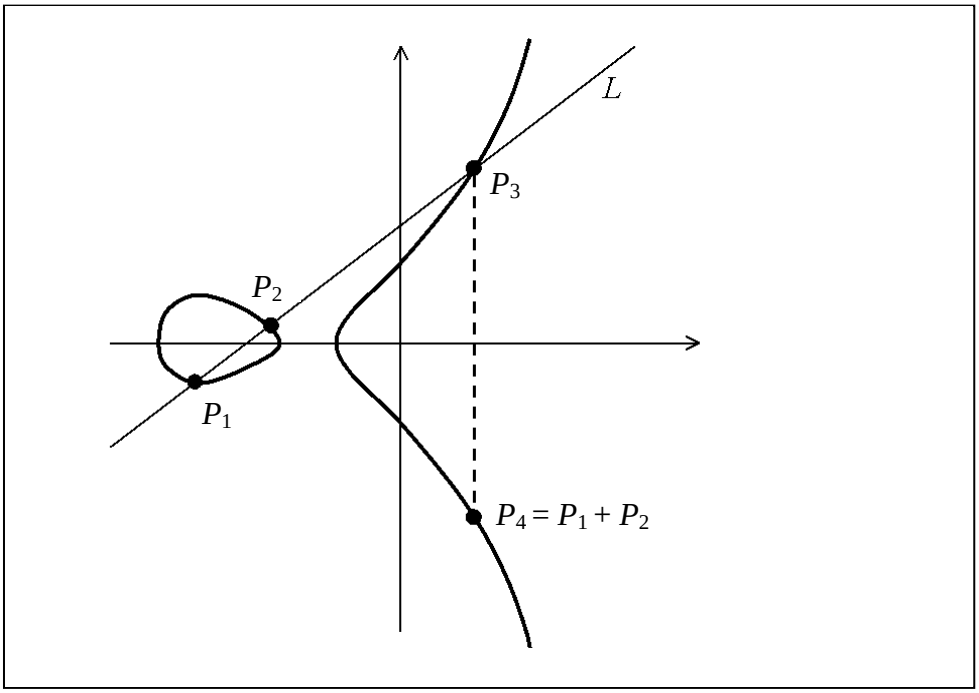

Figure 2.5: Elliptic curve

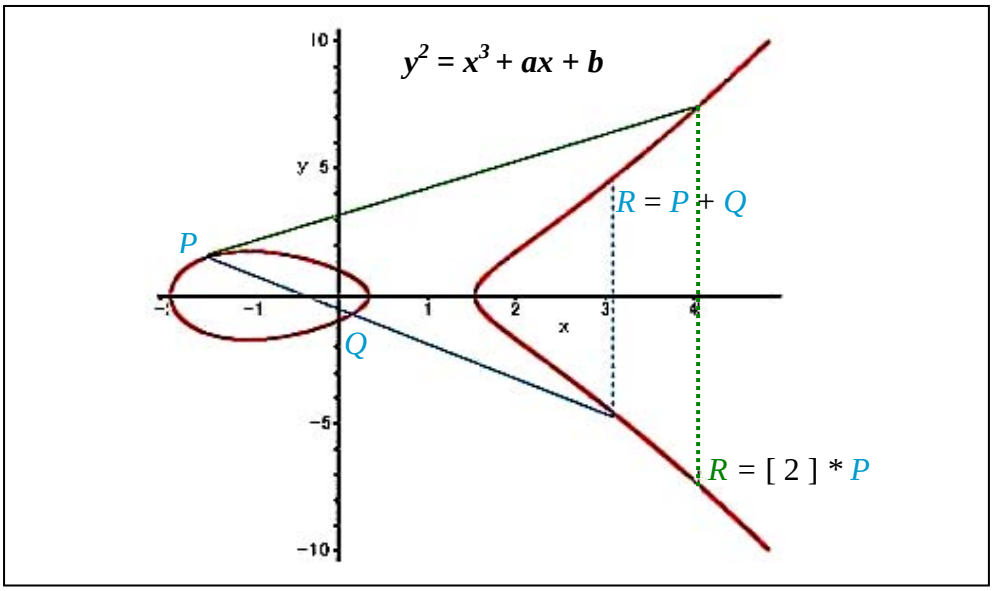

Figure 2.6: Elliptic curve addition and doubling

Identity Element: Point *O* at infinity, as conceming this elliptic curve addition, takes the usual role of the number "zero". In other words $P + O = O + P = P$ holds.

Discrete Logarithm on Elliptic Curves

Although most DL-based protocols were originally defined on the multiplicative group of a finite field F^*_q, the discrete logarithm problem (and Diffie-Hellman problems) can of course be defined on any group. The protocols can thus be translated in terms of groups that possibly allow better security or more efficient arithmetic. In some groups, however, taking discrete logarithms is easy, for example in the additive group of a finite field. Obviously, such groups are not suitable for cryptographic purposes, as security is based on the hardness of DL. Fortunately, there also exist groups in which solving the discrete logarithm problem is believed to be harder than in F^*_q, where the Index Calculus Method provides a sub exponential algorithm. The group of points on an elliptic curve is an example of such a group.

2.4 Diffie-Hellman Problems

With the group G_1 described in section 2.3, we can define the following hard cryptographic problem applicable to our proposed scheme.

- *Discrete Logarithm (DL) Problem:* Given $P, Q \in G_1$, find an integer n such that $P=nQ$ whenever such integer exists.
- *Computational Diffie-Hellman (CDH) Problem:* Given a triple $(P, aP, bP) \in G_1$ for $a, b \in Z_q^*$, find the element abP.
- *Decision Diffie-Hellman (DDH) problem:* Given a quadruple $(P, aP, bP, cP) \in G_1$ for $a, b, c \in Z_q^*$, decide whether $c=ab \bmod q$ or not.

- *Gap Diffie-Hellman (GDH) Problem:* A class of problems where the CDH problem is hard but DDH problem is easy.
- *Bilinear Diffie-Hellman (BDH) Problem:* Given a quadruple $(P, aP, bP, cP) \in G_1$ for some $a, b, c \in Z_q^*$, compute $\tilde{e}(P,P)^{abc}$.

Groups where the CDH problem is hard but DDH problem is easy are called GAP Diffie-Hellman (GDH) groups. Details about GDH groups can be found in [34], [35], [36]. There are also some other Diffie-Hellman Problems which are not associated with our proposed protocol. Details about other Deffie-Hellman problems can be found in ref. [37].

CHAPTER 3

ANONYMOUS PROTOCOLS AND COMPARISON ANALYSIS

In this chapter we discuss the achieved properties of the recent existing protocols and make a comparison analysis among them as well as our proposed protocols AODPR and RIOMO. We give an emphasis to the security properties which we discussed in chapter 2.

3.1 Related Research on Anonymous Routing

There are some recent *topology-based* anonymous protocols such as SDDR [17], ANODR [19], MASK [22], and also in *position-based* anonymous protocol namely AO2P [16], that all are taking care of privacy in MANETs. Here we are discussing the key points of these protocols.

SDDR: Secure dynamic distributed routing algorithm (SDDR) is a distributed path construction protocol for anonymizing communication in wireless ad hoc networks. The protocol does not require the source node to gather and store information about the network topology. Instead, the source node initiates a broadcast message intended for a selected destination node. Intermediate nodes insert their identification (IDs) and a session key into the message and forward copies of this message to their neighbors until the message gets to its intended receiver. Intermediate nodes encrypt this

information before adding it to the message, and only the intended receiver node is able to decrypt it. Once the receiver node receives the message, it retrieves from the message the information about all intermediate nodes, encapsulates this information in a multi-layered message, and sends it along a reverse path in the dissemination tree back to the source node. Each intermediate node along the reverse path removes one encrypted layer from the message, and forwards the message to its ancestor node until the message reaches the source node. When the protocol terminates, the source node ends-up with information about all the intermediate nodes on the discovered route as well as the session keys to encrypt the data transmitted through each of these nodes. The multicast mechanism and the layered encryption used in the protocol ensure the anonymity of the sender and receiver nodes.

ANODR: In ANODR the anonymous route discovery process establishes an on-demand route between a source and its destination. Each hop in route is associated with a *random route pseudonym.* The design of route pseudonym is based on a network security concept called *"Broadcast with trapdoor information"*. Trapdoor information is a security concept that has been widely used in encryption and authentication schemes.

There are three types of ANODR route discovery, which are described as follows:

1) ***ANODR-PO*** (Anonymous route discovery – public key protected)
   RREQ phase: Each *RREQ* forwarding node X prepends the incoming hop to the PO structure, encrypts the result with its own public key PK_X, then broadcasts the *RREQ* locally.
   RREP phase: When the destination receives an *RREQ* packet, the embedded PO structure is a valid onion to establish an anonymous route towards the source.
2) **ANODR-BO** (Anonymous route discovery – Boomerang Onion)

RREQ phase: When intermediate forwarding node X sees an *RREQ* packet, it prepends the incoming hop to the boomerang onion, encrypts the result with a random symmetric key K_X, then broadcasts the *RREQ* locally.

RREP phase: The boomerang onion will be bounced back by the destination. Like the public key version, when node X sees an *RREP* packet, it strips a layer of the boomerang onion and locally broadcasts the modified *RREP* packet. Finally the source will receive the boomerang onion it originally sent out.

3) **ANODR-TBO** (Anonymous route discovery – Trapdoor Boomerang Onion)

RREQ phase: When intermediate forwarding node X sees an *RREQ* packet, it embeds a random nonce NX to the boomerang onion (this nonce is not a route pseudonym nonce), encrypts the result with a random symmetric key K_X, then broadcasts the RREQ locally. The trapdoor information consists of N_X and K_X, and is only known to X.

RREP phase: The boomerang onion will be bounced back by the destination. After each local *RREP* broadcast, only the next hop (i.e., the previous hop in *RREQ* phase) can correctly open the trapdoor it made in the *RREQ* phase.

MASK: In MASK, nodes use pseudonyms instead of their real identifiers in the routing process. If one node uses one pseudonym all the time, it won't help to defend against traffic analysis because the pseudonym will be analyzed the same way as the real identifier. Therefore, each node should use dynamically changing pseudonyms. For this purpose, the trusted authority (TA) furnishes each node ID_i with a **sufficiently large set** PS_i of collision-resistant pseudonyms and a corresponding secret point set as $S_i = gH_1(PS_i) = \{ S_{i,j} \} =$

{ $gH_1(PS_{i,j}) \in G_1$} ($1 \leq j \leq |PS_i|$). Since the discrete logarithm problem (DLP) is believed to be hard in G_1, given one pseudonym and secret point pair < $PS_{i,j}$, $S_{i,j}$>, adversaries cannot deduce the system master key with non-negligible probability. In addition, there is no one but the TA can link a given pseudonym to a particular node or identity, or deduce the corresponding secret point with non-negligible probability.

AO2P: AO2P is discussed in terms of route discovery and receiver classification procedure.

AO2P Route Discovery:

- CSMA/CA is used as the channel access mechanism for most control messages.
- A source obtains the position of destination. It then generate a route request (rreq) for route discovery.
- A sender of rreq (a source or a forwarder) generates a pseudo name. After sensing the channel to be idle for a *DIFS*, it transmits the rreq that carries the position of the destination and the distance from itself to the destination.
- Nodes receiving the rreq contend to send a hop reply (hrep) to the previous hop following a receiver contention mechanism. The winner of the contention is determined by position information.
- Upon receiving a hrep, the sender confirms the successful contention by replying the winner with a confirmation message (cnfm) after a *SIFS*.
- Upon receiving the cnfm, the winner of the contender will be the next hop and reply with an ack after a *SIFS*. It then generates a temporary pseudo name for this session and transmits the rreq.
- When detecting a hrep collision, the sender retransmits the rreq after a *SIFS*.

- The process is repeated until the destination is reached. The destination replies with a route reply message (rrep) to the source following the reverse route (i.e., nodes in pseudo names) and indicates the completion for the route discovery.

AO2P Receiver Classification:

- A node receiving a rreq, i.e., a receiver, assigns itself to a certain node class based on if it is the next hop, how closer it can carry the packet to the destination.
- A receiver that can carry the rreq closer to the destination will be assigned to a class of a higher priority.
- Destination node has the highest priority

3.2 Comparison and Analysis

In *position-based* routing strategy to design an anonymous routing protocol there is an anonymous protocol, called AO2P [16], that does not ensure location privacy, because the distance is always kept in the *RRQ* packet, thus any intermediate node can estimate the distance form it to the source and/or destination. In our proposed protocol AODPR, the position of the destination is encrypted with a common key of nodes, and this encrypted position is used for the routing. Information is thus not disclosed to nodes not composing the ad-hoc network. In AODPR, a route is discovered by a dynamic handshake mechanism, which dynamically determines the next hop. For this purpose, a route-request message is sent from the source towards the position of the destination. In AO2P; by using a receiver contention mechanism route discovery procedure is performed.

In ref. [17], a secure dynamic distributed topology-based routing algorithm (SDDR) based on the onion-routing protocol [18] for ad-hoc wireless networks have been proposed. The anonymity-related properties

achieved with this algorithm include weak location privacy and route anonymity. However, it ignores one important part of privacy in mobile ad-hoc networks, namely, identity anonymity, and it cannot provide strong location privacy.

In ref. [19], Kong et al. design an Anonymous On-Demand Routing (ANODR) based on topology. Similar to Hordes [20], ANODR also applies multicast/broadcast to improve recipient anonymity. ANODR is an on-demand protocol, and is based on trapdoor information in the broadcast. These features are not discussed in regards to Hordes' [20] multicast mechanism.

Compared to [17], ANODR gives a more comprehensive analysis of the anonymity and security properties, and provide detailed simulation results. In addition, ANODR is more efficient than SDDR at the data-transmission stage. However, similar to SDDR in [17], ANODR does not provide identity anonymity and strong location privacy.

Another approach of *topology-based* anonymous communication based on pairing-based cryptography proposed by Zhang *et al.,* [22], called MASK. In MASK, system administrator generates a large set of pseudo IDs for every node, that is every node has a fixed pseudo ID set and it should be large enough set, otherwise there is a chance of finding pseudonym linking by the intruders. As a result anonymity of the nodes decrease and it fails to full fill its target. If the pseudo ID set for a node is small then anonymity property lose of the MASK protocol, because every node has to repeat its pseudo IDs after finishing one round of all its pseudo IDs. Thus pseudo IDs work as real IDs and intruders able to identify each node. So, to keep strong anonymity in MASK, every node should have to manage an extremely large enough number of pseudo IDs set provided by the system administrator, which is costly for ad-hoc network communication in terms of extra task for nodes, namely IDs maintenance cost.

Concerning *topology-based* protocols in MANETS; and to achieve strong communication anonymity and security, an anonymous on-demand routing protocol, called RIOMO, is proposed. In RIOMO, every node can generate its own pseudo IDs dynamically based-on pairing-based cryptography and random numbers; also nodes can generate their pseudo IDs independently without making communication with the system administrator. Thus pseudo IDs maintenance cost is reduced compared to MASK by Zhang et al., [22].

Concerning the rushing attack, an existing on-demand routing protocol, such as AODV [7], DSR [8], location-aided routing (LAR) [38], Ariadne [39], secure AODV [40], a secure routing protocol for ad-hoc networks (ARAN) [41], AODV secured with statistically unique and cryptographically verifiable (SUCV) [42] and secure routing protocol (SRP) [43] are all susceptible to rushing attack.

3.3 Our Result and Comparison with Other Protocols

Although SDDR and ANODR are topology-based, these protocols guarantee many privacy properties, as shown in Table 3.1. The proposed AODPR and other two protocols are described in Tables 3.1 and Table 3.2 with respect to security and routing strategies, respectively.

Table 3.1: Comparison of Security-related properties of AODPR with others protocols

Routing protocol / Sec. properties	SDDR	ANODR	**AODPR (proposed)**
Identity privacy *	√	×	√
Identity privacy **	×	√	√
Weak location privacy	√	√	√
Strong location privacy	×	×	√
Route anonymity	×	√	√
DoS attacks	××	××	√√
Wormhole attacks	√√	√√	√√
Rushing attacks	√√	√√	√√

×: Not achieved √: Achieved
××: Not protected √√: Protected
* : Identity privacy of source and destination
**: Identity privacy of forwarding nodes in route

Table 3.2: Comparison of routing strategies of AODPR with others protocols

Routing protocol / Strategy		SDDR	ANODR	**AODPR (Proposed)**
Routing strategy	Broadcast	Yes	Yes	Yes
	RREQ	Flooding	Flooding	Convergence

RREQ: Route request packet
Flooding: Network-wide flooding process
Convergence: Converging on a destination

Comparison analysis of proposed protocol, RIOMIO, with SDDR and ANODR are given in Table 3.3, and Table 3.4.

Table 3.3: Comparison of Anonymity-related properties of RIOMO with others protocols

Routing protocol / Anonymity properties	SDDR	ANODR	**RIOMO (proposed)**
Identity privacy *	√		√
Identity privacy **		√	√
Weak location privacy	√	√	√
Strong location privacy			√
Route anonymity		√	√

√: Achieved (blank): Not achieved
* : Identity privacy of source and destination
**: Identity privacy of forwarding nodes in route

Table 3.4: Comparison of Security-related properties of RIOMO with others protocols

Routing protocol / Security properties	SDDR	ANODR	**RIOMO (proposed)**
DoS attacks			√
Wormhole attacks	√	√	√
Rushing attacks	√	√	√

√: Protected (blank): Not protected

CHAPTER 4

PROPOSED PROTOCOL: ANONYMOUS ON-DEMAND POSITION-BASED ROUTING (AODPR)

4.1 Fundamentals

In this section basic fundamental for AODPR is described. AODPR assumes available secure position service system to maintain position of the nodes. So, at first position management is described. A dynamic handshaking is defined for route discovery and it is discussed in this section also.

4.1.1 Position management

Known position-based routing protocols [21, 44, 45, 16] use a position/location management scheme, called a virtual home region-based distributed secure position service (DISPOSER). In this scheme, each node has its own virtual home region (VHR) [45], which is a geographical region around a center specific to the node. The center is fixed center and anyone can identify it by taking a concatenation of two publicly known values, namely, the node's ID and position information regarding the center of the whole network, as input to a publicly known hash function. There are position servers PSs for each node in the network. PSs of a node N exist only inside the VHR of N and manage position information of N as follows. To report the

position of N to its PSs, N executes a region-based broadcast [45] in the VHR if N stays inside its VHR. If N stays out of its VHR, N sends a packet containing position information of N and the center of N. The latter position information is used for determining which node forwards the packet. Once the packet reaches a node in the VHR, the node executes a region-based broadcast. After the region-based broadcast the PSs can store the latest position information of N. To retrieve position information of N, a source sends a request packet in the direction of the center of N. When the packet reaches a node in the VHR of N, the node executes a sequential searching method [45] and finally the packet reaches one of the PSs. The source authenticates itself to the PS, and then the PS provides the required position information. Using this position information, the source can establish a path from him to the destination. PSs are determined from the node density, the size of the VHR, the robustness of the system, and so on, and the number of the PSs is set in an appropriate value that makes the sequential search more cost-effective than the region-based broadcast and the management cost of the position information low enough. More details on the VHR are described in [21, 45].

The PS of our proposed scheme has an additional property: PS provides a source with additional information to enhance the authenticity and secrecy of services provided by the PS. Before describing this scheme, we define two notations: *Position information* denotes a pair composed of position and time, and legitimate nodes denote nodes which have registered with PS and received a common key C_K form PS.

In contrast to ordinary PS, our PS provides a source with a common key C_K for all legitimate nodes, public key PK of the destination, *position information* of the destination, authentication information *Auth*, and a *Token*.

When a node joins a network, it is registered the PS and gets a common key C_K and a pair of public key PK / secret key SK from the PS.

When a node updates its *position information* and sends it to the PS, it generates a *random number* and sends it together with its *position information* to the PS. This *random number* is used for generating *Auth*, where *Auth* = [H_1 (Destination's *Position*, Destination's *random number*)] and H_1 is a global hash function. The notation A=[B, C, ..., Z] means variable A is substituted by the concatenation of B, C, ..., Z. Later, at the route discovery phase *Auth* is used for authenticating the destination to the source.

To obtain the *position information* of the destination from the PS, the source has to send a signed position request to PS with a *route-request sequence number RRQSeqNo*. After verification of the signature, the PS responds to the source's request with the *position information* of the destination, *Auth*, public key P_K of the destination, and a *Token* defined as *Token*=[H_{PS}(Sender Temp ID, Receiver Temp ID), Time, *RRQSeqNo*], where H_{PS} is a local hash function defined by the PS. *Position information* is used for generating the temporary Identifier Temp ID. In contrast, *Position* is used only for routing, and it is encrypted by C_K in the route- request phase.

A sender keeps *Auth* received from the PS for a session of communication. At the last phase of the route-discovery procedure, destination will reply with a *route-reply message RRPMsg* for its authentication to the sender: $RRPMsg = [Sig_{SK_{Dest}}(Auth)]$, where Sig_{SK} is a digital signature function under secret key *SK*, and SK_{Dest} is the SK of the public/ secret key pair of the destination. With this *RRPMsg* the sender authenticates the destination.

A *Token* is sent in the last phase of data transmission to the destination. At the end of the communication, the destination sends this *Token* to PS, so that PS can determine whether the communication between the source and the destination is valid. If a node takes the *position information* of the destination and does not make a data transmission, then PS will not supply any further position information to that node.

4.1.2 Dynamic handshaking

A kind of handshaking defined, called dynamic handshaking, which is established from the ending point to the beginning point, is defined here as shown in Figure 4.1. At first, node A sends a signal for node D via B. B will response to A after getting a response from C. That means A will wait for a certain time. The whole handshaking process is performed from the ending to the beginning.

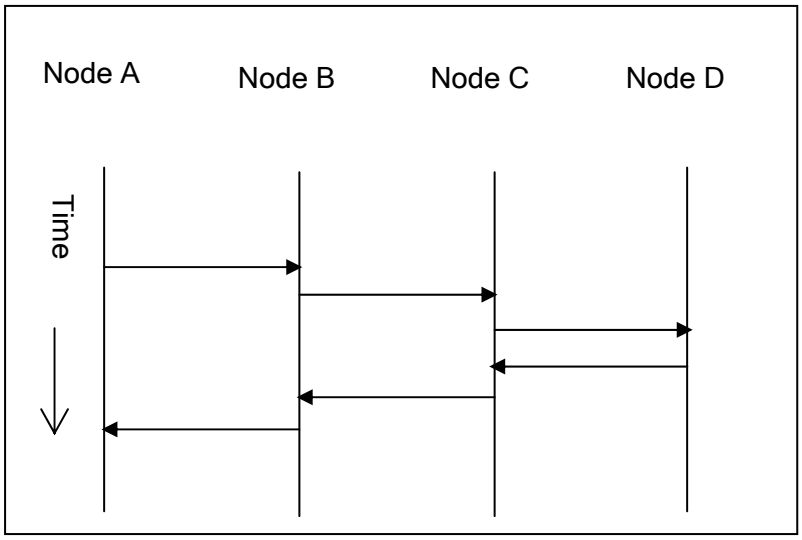

Figure 4.1: Dynamic handshaking

4.1.3 Control packets

Three control packets are used for route discovery of AODPR: *Route Request Packet RRQ*, *Route Reply Packet RRP* and Fail Packet *Fail*. These packets are described in *Appendix*. Here only a few fields of the *RRQ* are described.

Sender Temp ID: For every session of communication, a source generates its temporary ID Temp ID, computed as Temp ID = [*H* (Position, Time, PK)], where *H* is a global hash function known to all legitimate nodes in the network, Position is the position of the source, Time is the present time, and PK is a public key of the source. Temp ID uniquely identifies the source in each session of communication and is dynamically changed from session to session and from hop to hop. When nodes staying within the sender's radio range receive the *RRQ* packet, they will become new senders or forwarders and update the Temp ID into their own Temp ID, which is generated in a similar way to that mentioned above.

For successful identification, the Temp ID should be unique for each session of communication. To this end, *H* should be collision resistant. Theoretically proven collision-resistant hash functions are slow; thus, in practice, hash functions that are expected to be collision-resistant, such as Message Digest algorithm 5 (MD5) [46] and Secure Hash Algorithm 1(SHA-1) [47], are used instead. The probability of finding a collision for MD5 w.r.t 128-bit output and that for SHA-1 w.r.t 160-bit output have been estimated as, on average, 2^{64} and 2^{80}, respectively. As long as these probabilities hold, it is difficult to find the same Temp ID for different nodes in each session of communication

Position of Destination (PD): The geographical position (X_T, Y_T) of the destination, taken from PS and encrypted by C_K.

Number of Hops (NH): NH is the minimum number of hops that an *RRQ* packet travels to find a route from the source to the destination. NH is estimated by the *source.* It is changed by the source when the source tries to find a route with a new estimation. It is also encrypted by C_K.

Temporary Number of Hops (Temp NH): At the beginning of route discovery, Temp NH is initiated as NH by the source, Temp NH = NH and it is encrypted with C_K by the source. After receiving the *RRQ* packet by

legitimate nodes, it is updated. Update means decrementing by *one*, i.e., Temp NH = Temp NH - 1. When the *RRQ* packet travels from node to node it is updated each time by each node. Moreover, the nodes perform encryption/decryption operations and vice-versa by C_K.

4.2 Protocol

AODPR protocol is described with the functionalities of the nodes here. At first parameter of network placements is given and later overview of the node functionalities are given.

4.2.1 Parameters description

In certain environments, such as stadiums, classrooms, disaster areas, and battle fields, node placements and their corresponding density can be defined as follows.

Quadratic placement means that a node is connected in its radio range with its neighbors in all four compass directions from its center (Figure 6.1) thus, their corresponding densities are approximated as $\mu_{quad} \approx \sqrt{n}/[\{\pi + (\sqrt{3}/2) + 1\} \times R^2]$, where n is the number of nodes to make the connection and R is the radius of the maximum radio-range coverage of each node of the ad-hoc network. When any node sends a packet within its radio range, the other nodes within its radio range can receive the packets. *Line placement* means that a node can be connected to any node in a line via intermediate nodes. *Least placement* means that a node can reach another node with just one connection to its neighbor (Figure 6.2).

At first, we describe the estimation of NH by the source for different placements of the nodes in the network. The source estimates NH on the basis

of the density of the nodes in the network, and NH is the highest when node density is the lowest and vice-versa. NH is thus proportional to $1/\mu$, where μ is the density of the nodes.

For *line placement,* NH=D/R, where R is the radius of the maximum radio-range coverage of each node of the ad-hoc network, D is the distance from the source to the destination, D= $\sqrt{(X_T - X_S)^2 + (Y_T - Y_S)^2}$, where (X_S, Y_S) and (X_T, Y_T) are the source's and destination's positions, respectively. In this placement, NH is the minimum number of hops, from the source to the destination, estimated by the source.

For μ_{qaud} it is assumed that NH=f(L,B)/R, where f is a linear function in L and B , length L is the horizontal distance from the source to destination, and breadth B is the vertical distance from the source to destination.

For *least placement,* it is assumed that NH=(k×g (C))/R, where k is a constant and a function of L/R or B/R; and g is an exponential function in circumference C of the area of the network. In this placement NH is the maximum number of hops, from the source to the destination.

4.2.2 Overview

The AODPR protocol is described in detail with respect to the functionalities of the nodes.

Source*:* The source sends a request to the PS for the position information of the destination when it wants to communicate with the destination. AODPR is thus an on-demand protocol. The source generates its own Temp ID, *RRQSeqNo* and estimates NH and the maximum number of hops.

After receiving the destination's position, the source estimates NH and assigns this NH to Temp NH. It then source sends an *RRQ* packet within its

radio range and waits to receive a *response*, which is either *RRP* or *Fail* during time 2×*TTL*, where *TTL* denotes *time to leave* and is estimated by the source from *TTL = (traveling time for one hop) × (number of hop).*

- If the source receives *RRP*, by decrypting *RRPMsg* of *RRP*, it tries to find a match with *Auth*. If a match is found, it stores the corresponding *RRQSeqNo,* NH, receiver's Temp ID and status (i.e., "yes") in its routing table. It then sends data encrypted by the destination's public key. Lastly sender sends *Token* to the destination so that destination can inform the PS of this communication.
- If it receives a *Fail* packet, it stores the corresponding *RRQSeqNo*, NH, and status ("no") to its routing table, and again tries with a new estimated NH.
- If it does not receive any *response* and *TTL* is exceeded, it stores *RRQSeqNo,* NH and status ("no") in its routing table, and again tries with a new estimated NH.

As a result of this procedure, if the source fails to find the destination with an estimated NH, it tries with the next estimated NH until it finds the route. In this way, it can try with the minimum to the maximum estimated NH. Moreover, the maximum number of hops can be varied for different placements.

Intermediate nodes or Forwarders: If a node receives a packet *RRQ* but it is not the destination it is a *forwarder* and becomes a new sender. Forwarder F generates its own Temp ID and calculates distance $D_r(F)$ between F and its destination T by $D_r(F) = \sqrt{(X_T - X_F)^2 + (Y_T - Y_F)^2}$ from the forwarder's position (X_F, Y_F) and destination's position (X_T, Y_T). F then updates Temp NH by Temp NH=Temp NH - 1. It compares this updated Temp NH with $D_r(F)/R$ and makes the following decision, as shown schematically in Figure 4.2.

- If $D_r(F)/R \leq$ Updated Temp NH, forwarder F forwards the packet to its radio region and keeps the route information.
- If $D_r(F)/R >$ Updated Temp NH, forwarder F discards the packets.

After forwarding a packet, the forwarder waits to receive a *response* for time $2\times TTL_1$, where TTL_1 is computed from TTL_1 = *(traveling time for one hop)* × *(updated number of hops).*

- If the forwarder receives *RRP*, it just forwards it on the reverse path and keeps the route information.

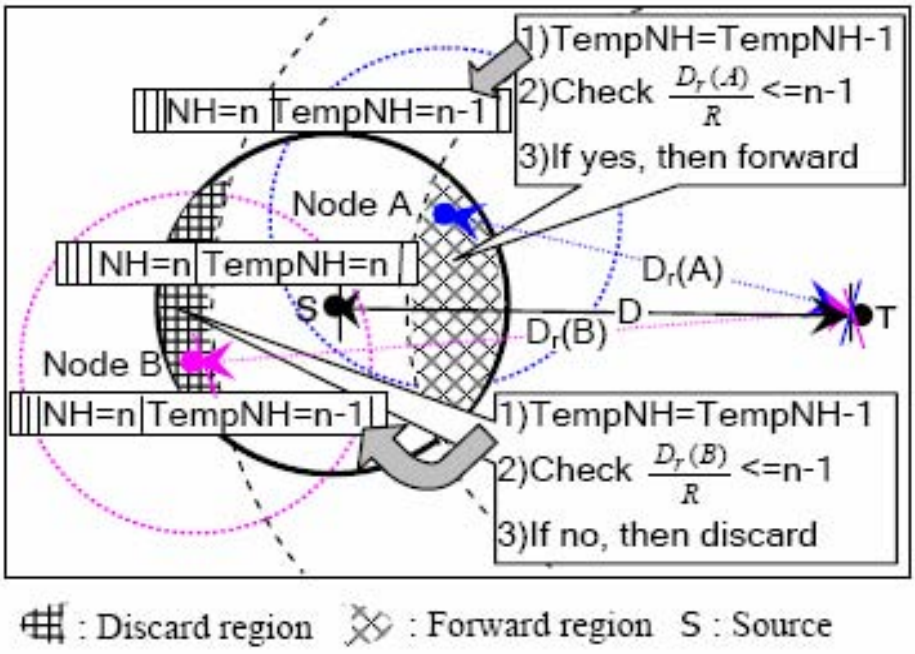

Figure 4.2: Packet forwarding or discarding in intermediate nodes.

- If the forwarder receives *Fail*, it also forwards it on the same reverse path and keeps the route information.
- If it does not receive any *response* and its waiting time exceeds TTL_1, it generates *Fail* and forwards it on the reverse path.

Destination: The destination checks EM of *RRQ* to confirm the destination of *RRQ.* Finally, it replies by *RRP* and keeps the route information.

4.3 Procedures

Carrier sense multiple access with collision avoidance (CSMA/CA) [48] is used as the channel-access mechanism for control messages. A sender (a source or a forwarder) of an *RRQ* transmits the *RRQ* after sensing the channel and finding idle time for a distributed inter frame space (DIFS). When there is a collision, the sender retransmits the *RRQ* after a short inter frame space (SIFS). The same procedure is applicable for any node for the *RRP* as well as *Fail*.

Initial procedure:

A source makes a signed position request to the PS, and receives required information C_K, destination's *position information, Auth, Token,* and PK of the destination from the PS.

Source's working procedure:

The source generates an *RRQ* and sends it to its radio region and waits to receive a *response* for time 2 × *TTL*.

If it receives a following *response*

- If source receives *RRP*, then it compares *Auth* with *RRPMsg* by decrypting it.
    - If it matches, then source sends data in the path and at last sends the *Token*.

- If it does not match, then source discards this *RRP* and estimates a new NH and again tries this procedure until it receives a valid *RRP*.

- If source receives a *Fail* packet within time 2×TTL, it estimates a new NH and again tries this procedure until it receives an *RRP that does not exceed the maximum number of hops for that environment*.

If the source does not receive any response and the waiting time exceeds 2×*TTL*, the source estimates a new NH and again tries the above procedure until it receives an *RRP*. The source repeats this procedure as long as the NH of its packet is smaller than the *maximum number of hops for that environment*.

Forwarder's or destination's working procedure:

On receiving an *RRQ,* a forwarder checks whether it is the destination or not.

If it is the destination, then it generates an *RRP* and sends this *RRP* on the reverse path.

If it is not the destination, then it forwards the *RRQ* and waits for time 2×TTL_1

- If the forwarder receives a *RRP,* it keeps the route information and sends it on the reverse path.
- If the forwarder receives *Fail,* then it keeps the route information and sends it on the reverse path.

If the waiting time for the forwarder exceeds 2×TTL_1 time, then the forwarder generates *Fail* and sends it on the reverse path.

4.4 Anonymity Achievement and Security Analysis

When senders or forwarders forward any packets, they generate a large bit random number and use parts of that random bit sequence corresponding to the number of encrypted fields of the packet, i.e., RRQ and RRP. The packets are described in the appendix. They also specify all the fields with a specific bit number. They then pad the fields with random bits and encrypt these fields. When a packet reaches a node, the node first decrypts it, extracts the random bits from the fields, and pads these fields with its own random bits. All the fields of a packet are thus changed. As a result, when the packet moves from node to node it appears new to the network. This procedure is applicable to all the encrypted fields of all the packets. Encryption and decryption are performed as necessary when a packet moves from node to node.

Identity Privacy: In AODPR the identities temp ID of the nodes are changing in each hop as a packet is forwarded. Location of destination is encrypted and padded with random bits. Also the temp ID is changed in each session of communication. So AODPR ensures identity privacy.

Location Privacy: The general concept of the current attacks on the location privacy is to observe the route request and route response packets and to estimate the distance between the source and the destination from the traveling information added to the packet, i.e., how many hops it travels. In contrast to existing anonymous ad-hoc routing protocols, there is no extra traveling information added to the packets in our scheme, as shown in Figure 4.3, and estimating the distance between the source and the destination is not possible in a straightforward way. No node knows anything about the location and identity of the other nodes, including the source, and it does not know from where a packet starts to travel in the network. Even though all legitimate

nodes can determine the distance from themselves to the destination and also know the temp ID of other nodes in the neighboring region, no one except the source can determine the distance from the source to the destination by using this information. Location privacy is thus achieved.

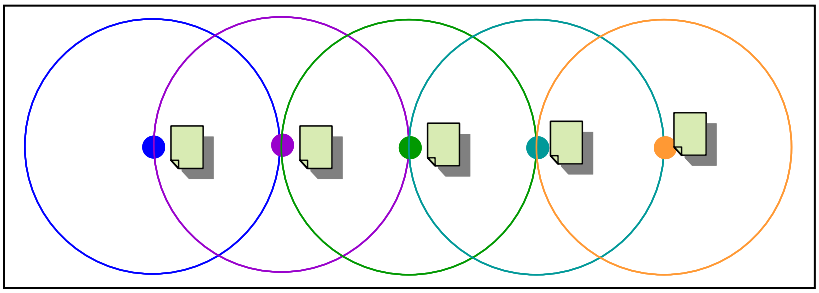

Figure 4.3: Location privacy model achieved by AODPR

Route Anonymity: Current attacks on route anonymity are based on traffic analysis [49]. The general theory behind these kinds of attacks is to trace or to find the path in which the packets are moving. For this purpose, a malicious node, mainly looks for unchangeable information i.e., common information in a packet, so that it can trace the movement of control packets. As a result, the adversaries can find or estimate the route from the source to the destination. In AODPR, all the control packets appear new in the network when packets moves form node to node as shown in Figure 4.4. So no one can trace the path of the route. Route anonymity is thus achieved.

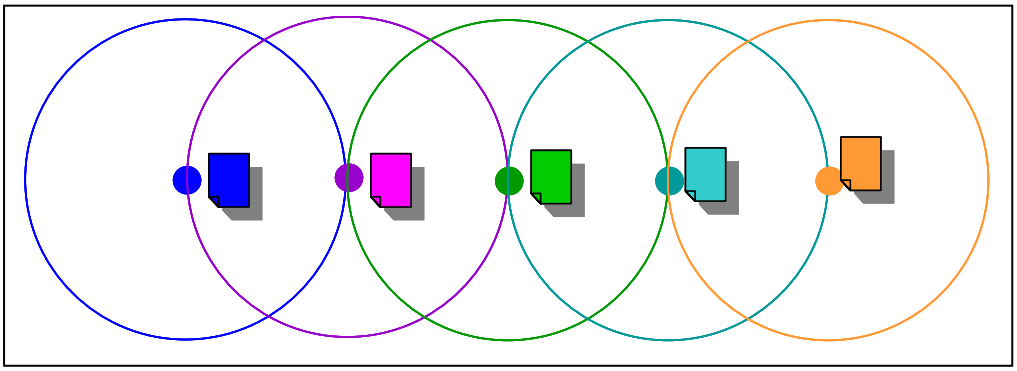

Figure 4.4: Anonymity model achieved by AODPR

DoS: Multiple adversaries cooperatively or one adversary with enough power can exhaust the resource of a specific target node as we discussed in chapter 2. To this end, adversaries need to identify a node and set that specific node as a target. In AODPR, identity privacy is achieved as discussed above and *DoS* can be protected.

Wormhole Attacks: In wormhole attack, there could be a long distance for a packet to travel for finding the route from the source to the destination as shown in Figure 2.3. In AODPR, the source and the forwarders wait for a *limited time, TTL or* TTL_1, for getting a response based on the estimated NH. If an attacker's response exceeds a *limited time,* it cannot be a forwarder within a routing path. If the attacker is a forwarder within a path limit and does not reply properly, this path no longer remains valid. The sender will try another path. A wormhole attack is therefore not effective in the case of AODPR.

Rushing Attack: Many existing on-demand routing protocols only forward the request that arrives first from each route discovery. In a rushing attack, the attacker exploits this property of the operation of route discovery, and establishes a rushing attack as shown in Figure 2.4. A more powerful rushing attacker may employ a wormhole to rush packets. By using the tunnel

of a wormhole attack, the attacker can introduce a rushing attack. As shown above, AODPR can prevent a wormhole attack. It is thus also robust against a rushing attack.

CHAPTER 5

PROPOSED PROTOCOL: ROUTING WITH INDETERMINATE OBJECTS FOR MOBILE AD-HOC NETWORKS OBSERVER (RIOMO)

5.1 Architecture and Design

In this section we discuss functionalities of the system administrator as well as of ordinary nodes.

System administrator does not take part in routing rather it has the following tasks during the boot strap of the network.

- Determines two groups G_1, G_2, of the same prime order q. We view G_1 as an additive group and G_2 as a multiplicative group as discussed in section 2.3.
- Determines bilinear map g: $G_1 \times G_1 \rightarrow G_2$, collision resistant cryptographic hash functions H_1 and H_2, where $H_1:\{0,1\}^* \rightarrow G_1$ mapping from arbitrary-length strings to points in G_1 and H_2: $\{0,1\}^* \rightarrow \{0,1\}^{\mu}$ mapping from arbitrary-length strings to μ-bit fixed length output.
- Generates system's secret $\boldsymbol{\acute{\omega}} \in Z_q^*$, where $Z_q^* = \{y \mid 1 \leq y \leq q-1\}$. Any one in the network does not know $\boldsymbol{\acute{\omega}}$ except system administrator. System administrator also uses this secret to generate the secret point of the non-adversary nodes.

Thus the system parameters $<G_1, G_2, g, H_1, H_2>$ are known to the non-adversary nodes. System administrator also provides the following parameters for nodes, regarding their IDs and secret points.

- Provides each node, a secret point SP_R, with respect to the node's real ID ID_R, which is defined as $SP_R = \boldsymbol{\acute{\omega}}\, H_1(ID_R)$. The Source and the destination use their corresponding secret point in the route discovery phase to authenticate each other. For a given set of $<ID_R, SP_R>$ no one can determine the system secret $\boldsymbol{\acute{\omega}}$ as we discussed in section 2.3 and 2.4.
- Provides each node a pseudo ID IDP_i, and their corresponding secret point SPP_i, which is defined as $SPP_i = \boldsymbol{\acute{\omega}} H_1(IDP_i)$; if $i \neq j$ then $IDP_i \neq IDP_j$ as well as $SPP_i \neq SPP_j$. For a given set of $<IDP_i, SPP_i>$ also no one can determine the system secret $\boldsymbol{\acute{\omega}}$.

With the above information any node can generate its own *pseudo IDs* and the corresponding *secret points* randomly in every session in communication. Let's check for a node, namely K; K has received its pseudo ID IDP_K and the corresponding secret point $SPP_K = \boldsymbol{\acute{\omega}} H_1(IDP_K)$ from the system administrator. Now, K is able to generate its own pseudo ID $ID_{PK} = R_K H_1(IDP_K)$, and the corresponding secret point of the generated pseudo ID $SP_{PK} = R_K SPP_K = R_K \boldsymbol{\acute{\omega}} H_1(IDP_K) = \boldsymbol{\acute{\omega}} R_K H_1(IDP_K) = \boldsymbol{\acute{\omega}} ID_{PK}$, where R_K is a random generated by K; this relation also holds the previous cited property in section 2.3 and 2.4, that no one can determine the system secret $\boldsymbol{\acute{\omega}}$ for a given set of pseudo ID and the corresponding secret point , $<ID_{PK}, SP_{PK}>$. Thus a node can generate its own pseudo IDs and corresponding secret points as its need.

5.2 Anonymous Neighbor Authentication

When a node wants to join to the network or moves to a new place, it has to authenticate within its neighbor nodes. Say, Alice has received her pseudo ID IDP_A, and the corresponding secret point SPP_A=**ώ**$H_1(IDP_A)$, i.e., <IDP_A, SPP_A> from the system administrator. She can join in the network by authenticating within her neighbor nodes or if she moves another place in the network different from her current place, she also needs to authenticate her within her neighbor. To avoid a *target oriented* attack; if Alice wants to change her pseudo ID different from her current pseudo ID without moving her place, she also needs to authenticate her current pseudo ID within her neighbor. For this purpose she generates pseudo ID ID_{PA}=$R_AH_1(IDP_A)$, corresponding secret point SP_{PA} = R_ASPP_A = R_A**ώ**$H_1(IDP_A)$= **ώ**$R_AH_1(IDP_A)$=**ώ**ID_{PA}, where R_A is a random generated by Alice; she also generates a random R_{RA} which is used to generate verification codes Ver_0* and Ver_1. Alice broadcasts her pseudo ID ID_{PA}, and a random R_{RA} within her neighbor region. One of her neighbor, let's say Bob, makes a response with his pseudo ID ID_{PB}, generated random R_{RB} and verification code Ver_0 as shown in Figure 5.1. If Alice is a valid node then Ver_0*=Ver_0, and Ver_1^*=Ver_1 thus she can be a member and she is identified as ID_{PA}, within her neighbor. Alice and Bob use their session key K_{AB}= g (SP_{PA}, ID_{PB}) = g (ID_{PA}, ID_{PB}) ^{ώ} and K_{BA} =g (SP_{PB}, ID_{PA}) =g(ID_{PB} , ID_{PA}) ^{ώ}; thus K_{AB}=K_{BA} corresponding their pseudo IDs, ID_{PA} and ID_{PB} respectively. No one within Alice's neighbor can recognize her as Alice because she is using her pseudo ID and she is changing her pseudo ID time to time. Thus the nodes can hide their IDs in the network and always seem new to each other. Any adversary node can not be a member within its neighbor, because it has to pass the verification code "? (Ver_1*= Ver_1)" which

is not possible to generate without the knowledge of the system secret. Similar way all nodes in the network can authenticate anonymously within their neighbors and generate their corresponding session key. Thus nodes in the network maintain their neighbor table with their pseudo IDs and corresponding session key.

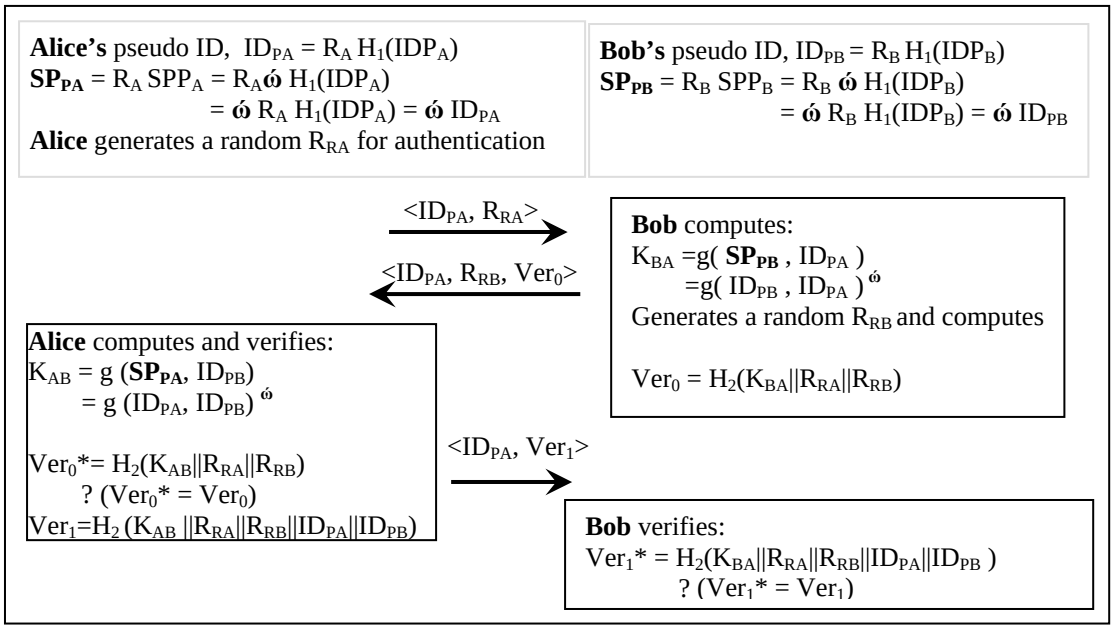

Figure 5.1: Anonymous neighbor authentication process for two neighbor nodes "Alice" and "Bob"

5.3 Control Packets

RIMIO uses route request packet *RRQ*, and route reply packet *RRP*, to find a route in the network. To discover a route and to receive a response it uses *RRQ* and *RRP* respectively.

RRQ

ID_{PSE}	*RRQSeqNO*	ID_S	ID_D

ID_{PSE}: Sender pseudo ID ID_{PSE}, it is the pseudo ID of the current sender. When sender broadcasts a *RRQ* packet it puts its own pseudo ID in this field. Thus $ID_{PSE} \neq ID_S$, but when the source is a sender then $ID_{PSE}=ID_{PSO}\neq ID_S$, here ID_S is the source's real ID and ID_{PSO} is the source's pseudo ID which we discussed in section 5.1.

RRQSeqNO: Route request sequence number is used for identifying each route-request and corresponding route-reply packet from each other. It is generated by the source uniquely when source wants to communicate with a destination. *RRSeqNO* $=H(ID_{PSO}||Time)$, where, H is a collision resistant hash function known to all non adversary nodes in the network, ID_{PSO} is a pseudo ID of the source, and Time is the calendar time when source generates *RRQ* packet. This field remains unchanged for the corresponding *RRP* generated by the destination.

ID_S: Source's ID ID_S, it is the source's real ID. Source generates a route request packet and puts its real ID in this field, and pseudo ID ID_{PSO}, in ID_{PSE} field; thus for source $ID_{PSE} =ID_{PSO}$ but $ID_{PSE} \neq ID_S$. It is used by the destination to make a sign in route reply packet.

ID_D: Destination's ID ID_D, it is the destination's real ID.

RRP

ID_{PSE}	ID_{PRE}	*RRQSeqNo*	$Sign_D$

ID_{PRE}: Receiver's pseudo ID; on the path from the destination to the source when *RRP* packet travels ID_{RPE} defines the next node who receives *RRP* packet.

$Sign_D$: Destination's Sign; when destination replies to source through intermediate nodes, it generates a sign, so that no one can forge. $Sign_D = H_2(K_{DS} \| RRQSeqNO)$, where K_{DS} is a session key between the source and the destination, and generated by the destination as $K_{DS} = g(\acute{\omega}H_1(ID_D),H_1(ID_S)) = g(H_1(ID_D),H_1(ID_S))^{\acute{\omega}}$.

Destination also uses its session key K_{DS}, to decrypt data, which sent by the source encrypted with source's session key K_{SD}, where $K_{SD} = g(\acute{\omega}H_1(ID_S),H_1(ID_D)) = g(H_1(ID_S),H_1(ID_D))^{\acute{\omega}}$.

5.4 Route Discovery and Route Reply

In route discovery and route response nodes maintain their corresponding table. When a node receives a *RRQ* packet it broadcasts within its neighbor and when it receives a *RRP* packet, it sends the *RRP* corresponding to the receiver. RIOMO is described in terms of its functionalities which are described below.

5.4.1 Route discovery

Every node in the network maintains its neighbor table with their pseudo IDs and corresponding session keys. When a source wants to communicate with a destination it generates a *RRQ* and broadcasts this *RRQ* within its neighbor to find a route, thus RIOMO is an on-demand routing protocol. By receiving a *RRQ*, a node checks ID_D and *RRQSeqNO*, of the *RRQ* and makes the following decisions:

- If the node is the destination i.e., ID_D matches with its real ID then it do the following tasks:

- It keeps < *RRQSeqNO*, ID_{PSE}> in its routing table; this ID_{PSE} becomes ID_{PRE} for *RRP*, generated by the destination. By replacing destination's own pseudo ID in the ID_{PSE} field of *RRQ*, it broadcasts *RRQ*, within its neighbor. The purpose of this extra broadcast is to make attackers fool.
- It generates a *RRP* with its own pseudo ID ID_{PSE}, receiver's pseudo ID ID_{PRE} already discussed above, makes a sign $Sign_D$ discussed in section 5.3 and sends to the receiver. Notice that *RRQSeqNO* is unchanged.

- If the node is not the destination and *RRQSeqNO*. is new, it keeps *RRQSeqNO*, corresponding pseudo ID ID_{PSE} in its routing table, this information <*RRQSeqNO*, ID_{PSE}> is used by the node in the route reply procedure; this ID_{PSE} becomes a receiver pseudo ID ID_{PRE} in the route reply procedure. The node becomes a new sender and it puts its own pseudo ID in the ID_{PSE} field of the *RRQ* and this *RRQ* within its region.

5.4.2 Route reply

It is just a reverse path traverse of a RRP explored by a RRQ. When a RRQ reaches to the destination it generates a *RRP* and forwards it in the reverse path as we discussed above. If a node receives a *RRP*, it checks *RRQSeqNO* in its routing table then updates receiver's pseudo ID ID_{PRE}, with an appropriate ID_{PSE} (i.e., from whom it receives the corresponding *RRQ* with the same *RRQSeqNO)*, and sends in the reverse path. If source receives a *RRP* it generates $Sign_S = H_2(K_{SD} \| RRQSeqNO)$ and verify $Sign_D$. If $Sign_S = Sign_D$ the source sends data in the explored path by encrypting with its session key K_{SD}.

5.4.3 Working procedure in brief

1. Nodes make authentication of their neighbor nodes and maintain their neighbor table. Thus only the trusted nodes can take part in authentication.
2. On Route discovery phase, source generates a *RRQ* and sends within its neighbor. If the destination is not within its neighbor then neighbor nodes become new sender. By replacing their own pseudo IDs broadcast within their own neighbor region. They also maintain this information in routing table as we discussed in section 5.4.
3. If the node is the destination it generates a *RRP* and sends in the reverse path as we discussed in section 5.4
4. Receiving *RRP*, source checks the authenticity of the destination, by comparing $Sign_S$ and $Sign_D$. If success then sends data in the explored path. Source and destination will use their corresponding session key for encryption and decryption as discussed in section 5.3 and 5.4.

5.5 Anonymity Achievement and Security Analysis

When an *RRQ* and *RRP* travel from node to, every node generates a large bit random sequence corresponding to the fields of *RRQ* and *RRP*. By extracting random bits from the fields of the packets, every node pads their own random bit sequence, and replaces their own pseudo IDs to the ID_{PSE} accordingly. Thus the packets appear new when it moves from node to node. Also the fields (except ID_{PSE}, ID_{PRE}) are encrypted with corresponding session keys, thus it is also protected from intruders.

Identity Privacy: In RIOMO the identities of the nodes are represented by their pseudo IDs which are changed by the nodes in each session of communication. Pseudo IDs are also generated by using random numbers, hash functions as we discussed in section 5.2, 5.3, also the control packets are encrypted so no one can recognize who is actual source and/or destination in a route request, route reply phase. Thus identity privacy of nodes is achieved in the network.

Location Privacy: If there is extra information added to control packets when the packets are forwarded form node to node; as shown in Figure 5.2; by observing the route request and the route response packets an attacker can estimation about the distance between the source and the destination. Thus, an attacker can set an attack regarding location privacy.

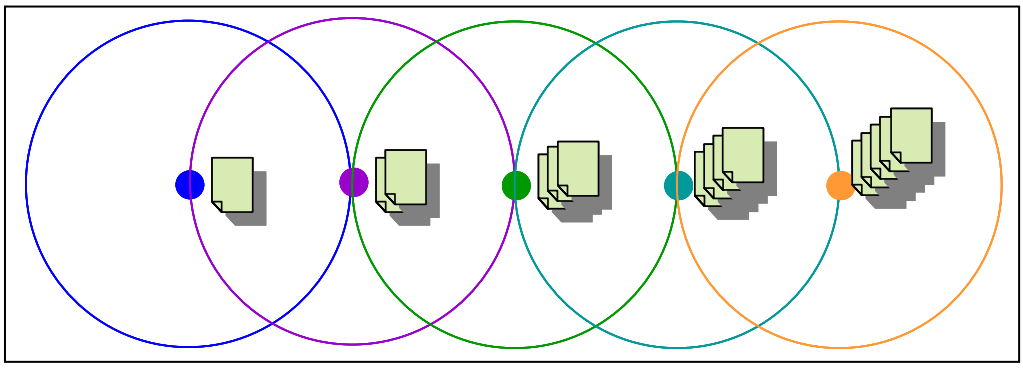

Figure 5.2: Attack model on location privacy

In our scheme, nodes do not know anything about the locations and identities of the other nodes in the network. Also there is no extra information is added when packets move from node to node, as shown in Figure 5.3. So, no nodes in the network can determine the distance from them to the source and to the destination; they also do not know about the starting point of a packet traveling in the network. Only in a session the nodes know pseudo IDs of its neighbor region. Thus RIOMO ensures location privacy.

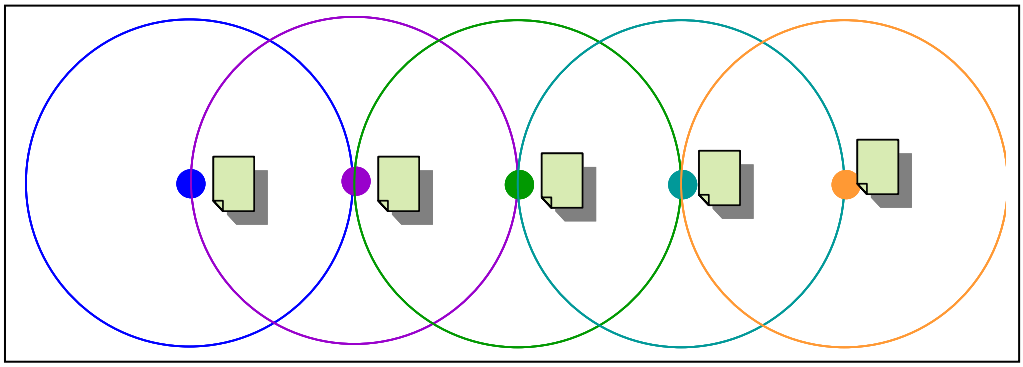

Figure 5.3: Location privacy model by RIOMO

Route Anonymity: Current attacks on route anonymity are based on traffic analysis [49]. The general theory behind these kinds' of attacks is to trace or to find a path in which packets are moving. For these purpose the malicious nodes mainly looks for common information which are not changing in a packet during movements of control packets. As a result, the adversaries can find or to estimate the route from source to the destination. In RIOMO all the control packets appear new (Figure 5.4) to the network, when it travels form node to node. Because every time random bits are extracted and padded during movements of the control packets as we discussed at the beginning of this section. Thus route anonymity is achieved of a path.

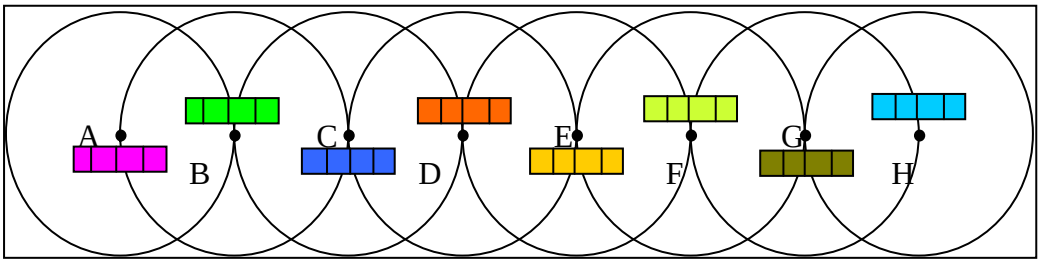

Figure 5.4: Anonymity model; when packets move from node to node the packet fields are always appearing new in the network.

DoS: According to the target of attack, multiple adversaries can co-operate or one adversary with enough power can target to a specific node to exhaust the resource of the node. For this purpose the adversaries try to identify a node and set a target to that specific node. In RIOMO identity privacy is achieved; so one can identify a node make a target to attack. Thus *DoS* can be protected.

Wormhole Attack: In wormhole attack an attacker records a packet in one location of the network and sends it to another location making a tunnel [23] between the attacker's nodes, later packet is retransmitted to the network under its control as we discussed in chapter 2. Thus there could be a long distance travel for a packet to find a route from the source to the destination. In RIOMO an attacker can not be a trusted member within its neighbor so it can not be an intermediate node in route discovery or route reply phase thus an attacker can not take part in the routing. So the affect of the wormhole attack is not effective in AODPR.

Rushing Attack: By using the tunnel of wormhole attack an attacker can introduce rushing attack to rush packets, as we discussed in chapter 2. Existing on-demand routing protocol, suffers from rushing attack, we already informed in chapter 3. We discussed that RIOMO can prevent wormhole attack so rushing attack is not effective in this protocol.

CHAPTER 6

PERFORMANCE ANALYSIS AND SIMULATION RESULT

In this chapter we discuss theoretical analysis of AODPR as well as RIOMO. We also highlight trade off of these protocols. Simulation result of AODPR is also given.

6.1 Theoretical Analysis of AODPR and RIOMO

In this section we will describe the theoretical properties of route exploration and reach-ability to reach any node in the network. Provided that the nodes should be connected with each other even at least a link. At first we will focus on AODPR and later RIOMO.

AODPR

In the case of AODPR, the source can determine the direct distance from him to any node connected in the network. Let the distance from the source to a node be *D*, so the number of hop given by $h=D/R$, where *R* is the radio-range coverage around a node. For route discovery, when a control packet travels from hop to hop, *h* is decremented by one. When a packet is forwarded to a specific node, the values of *h* will thus converge to a smaller value than its

previous value. Let *t* be the time a packet needs to travel *h* number of hops, within time *2× t,* the source will receive a response. If the source does not receive any response, it will estimate new hop h_1 and will wait for a corresponding traveling time $2\times t_1$. Thus, by consecutive estimation of new hops, the source reaches to the goal, as long as there is at least one path to reach the goal. If the density of the network is more than the quadratic-placement density μ_{quad} (Figure 6.1), it can reach the goal directly. If there is a shield on the path, it is also informed to the source by sending a fail packet after a certain amount of time. The source therefore estimates a new hop number by increasing its value more than in the previous attempts. If the source fails again, it will try as previously with a new estimate. If there is at least one path from the source to a node, then it can be found out, and successful communication is accomplished.

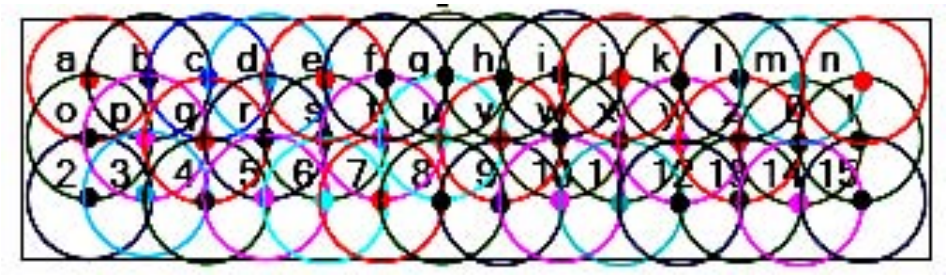

Figure 6.1: Quad-placement-connected network.

If the nodes in the network are at least-connected as shown in Figure 6.2, the maximum hop count to reach the goal is *n-1,* where *n* denotes the number of nodes in a network. Let us consider a path from node **a** to **z**, as an example path. At first **a** will calculate $D_r(a)$ from node **a** to **z** and also estimates NH, so that the packet travels according to the protocol for this NH. If the relation $D_r(F)/R >$ Updated Temp NH holds for a node in the path, that node discards the packet. After that, node **a** sends the packet with a new estimated NH,

which is a value greater than the old NH. Either with current estimated NH or a new estimated NH on the consecutive estimation of NH, the relation $D_r(F)/R$ > Updated Temp NH does not hold for that node any more and the node finally forwards the packet. As long as the NH of a packet from **a** is smaller than the maximum hop count, this procedure will continue. By taking an appropriate value for the maximum hop count, the packet can reach from node **a** to node **z**. The simulation results of least connected nodes in a network are given in section 6.2 with a different estimation of NH.

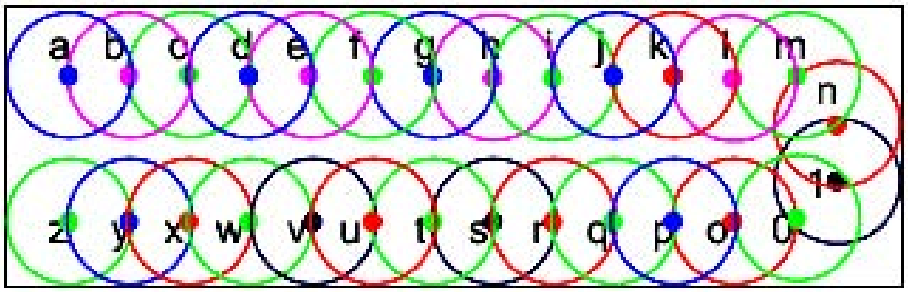

Figure 6.2: Least-placement-connected network.

RIOMO

In case of RIOMO, the route discovery procedure is a network wide flooding. So, within the radio-range coverage, *R*, of a node, data is broadcasted and duplicates of a packet to all neighboring nodes in the network. For route discovery many copies of the original data are generated during the flooding phase, and the destination users can double check the correct reception of the original data. It is also a robust method because no matter how severely the network is damaged, it can guarantee at least one copy of the data will be transmitted to the destination, provided a path is available.

6.2 Simulation Result

The reach ability in a network with least placement was simulated by varying the number of nodes, as shown in Figure 6.2, under a C++ programming environment. The graph shows the number of trials with respect to the number of nodes, in different estimation. For all the estimation methods the source at first initializes NH= D/ R. With this initial value the source tries to reach the destination. If the source fails, it estimates a new NH value and tries to reach to the goal with this value. Each time the source tries to reach the goal, the trial number is counted. For estimating NH value, we experimented with seven estimation functions. For all the estimation functions the *estimation value* is initialized by NH = D/R. These functions are mainly defined in two ways, (i) linear or (ii) exponential described as follows.

Estimation by linear I (I=1 to 5): After initializing the estimation value, it is incremented by I, so *estimation value=estimation value + I*. Detailed results for various I (I=1 to 5) are shown in Figure 6.3.

Estimation by exponential I (I=1, 2): After initializing the estimation value, it is incremented as a power, so *estimation value=(estimation value)*$^{I+1}$. When I =1, the source tries four times for 21 numbers of nodes to reach the goal and for 51 numbers of nodes, it tries four times, but the trial value for 5 to 15 numbers of nodes differs from the previous value and it is 3. When I=2, the source tries three times to reach the goal for 21 numbers of nodes, and for 51 numbers of nodes, it also tries three times and it remains constant from any number of nodes from 5 to 51. Exponential 2 is thus the best estimation for a least-placement-connected network.

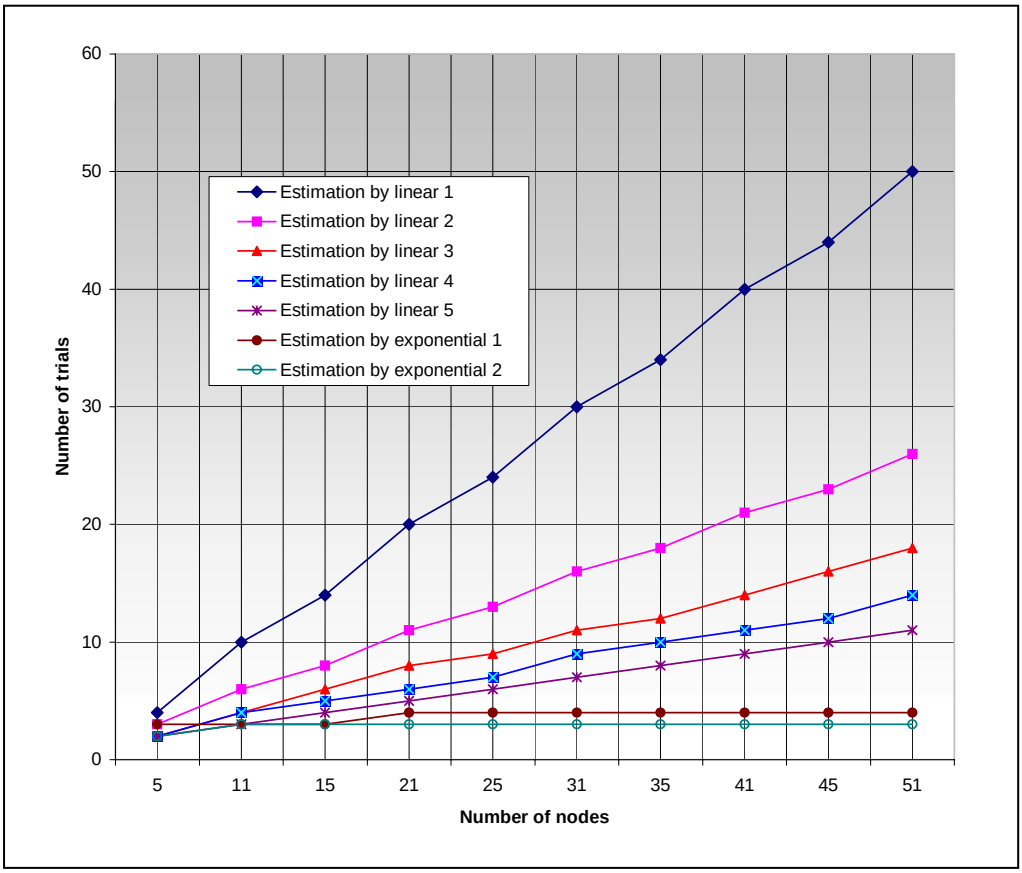

Figure 6.3: Number of trials for different estimation methods to find a route for different numbers of nodes in a least-placement-connected network.

6.3 Trade Off

AODPR

In an ad-hoc security routing protocol, the most expensive operation is the public key operation [50]. To guarantee the anonymity in the AODPR, every node generates its Temp ID, which is a hash computation, and a random bit corresponding to the fields of the packets, and it finally performs symmetric encryption/decryption of the fields. These computations are not more

computationally complex than those of some other ad-hoc security routing protocol [51].

To guarantee the anonymity in AODPR every node generates Temp ID and for that they should compute the following operations which are not heavy cryptographic computation compared to other existing protocols.

- Hash Computation
- Random bit generation
- Symmetric encryption/decryption

RIOMO

To guarantee the anonymity in RIOMO every node generates Pseudo ID and each node generates it from only one ID; for that they should compute the following operations which are not heavy cryptographic computation compared to other existing protocols.

- Hash Computation
- A pairing computation
- Random bit generation

CHAPTER 7

CONCLUDING REMARKS

Communication in mobile ad-hoc networks can be classified basically in two groups with respect to the location of nodes in network, namely *position-based* and *topology-based*. Since nodes in mobile ad-hoc networks move dynamically, adversaries cannot conduct active attacks without knowing the location or identity of nodes. Therefore adversaries want to know the location or identity of the nodes to conduct active attack. Practically malicious nodes conduct traffic analysis passively first and later set active attacks. However, to avoid such attacks nodes want to protect their location and/ or identity. Thus, anonymous communication becomes an essential factor in securing mobile ad-hoc network routing. So, researches on protecting node identities and preventing target oriented attacks have been considered. As a result two anonymous protocols namely Anonymous On-demand Position-based Routing, AODPR, and Routing with Indeterminate Objects for Mobile ad-hoc networks Observer, RIOMO, have been proposed for *position-based* as well as for *topology-based* respectively.

Existing protocol in *position-based* routing strategy does not provide location privacy. AODPR provides maximum of the privacy properties especially, node identity, route anonymity, location privacy and it is robust against most known attacks. To this end nodes generate temporary identifier, Temp ID, by computing cryptographic hash computation, and random number generation. For successful identification, Temp ID should be unique for each session of communication. So, hash function should be collision resistant. As long as the probability of finding a collision is negligible, it is difficult to find

the same Temp ID for different nodes in each session of communication. In terms of cryptographic computation it computes hash computation, generates random bit and performs symmetric encryption/ decryption.

Existing *topology-based* anonymous protocols [17], [19], [22] do not ensure maximum of the security and privacy related properties. Furthermore in MASK [22], anonymity depends on fixed large pseudo IDs set. So, every node has to perform extra task to maintain pseudo IDs, which is costly in terms of ad-hoc mobile communication. Therefore, to reduce pseudo IDs maintenances cost and ensure maximum privacy properties RIOMO is proposed. To this end, pseudo IDs are generated by the nodes dynamically form a pseudo ID, provided by the system administrator. Thus every node has to maintain only a pseudo ID and maintenance cost is reduced.

AODPR assumes secure position service system, so as long as position service system is fair it can maintain anonymous properties. Thus AODPR partially depend on this service system. Next and further research in position based scheme could be anonymous routing without any position service.

RIOMO also assumes that administrator should be fair in terms of its system secret; otherwise the security properties will lose of the protocol.

According to cryptographic computations, in both cases of *position-based* and *topology-based* schemes, energy consumptions are considered as future research. In addition degree of anonymity evaluation, achieved by AODPR and RIOMO protocols are also considered as future work.

Selfish and malicious node detection is still an open problem for the anonymous routing procedure in mobile ad-hoc networks.

APPENDIX

A. Control packets of AODPR

Here packets are described. Common key C_K is used for encryption and decryption by all legitimate nodes. E_{C_K} : means encryption with C_K.

A.1. Route Request Packet *(RRQ)*

Sender Temp ID	E_{C_K} (*RRQSeqNo*)	E_{C_K} (PD)	E_{C_K} (NH)	E_{C_K} (Temp NH)	E_{C_K} (EM)

For construction purposes when senders or forwarders forward any packet, they generate a large bit random number and make parts of that random bit corresponding to the number of fields of the packet. And they specify all the fields with a specific bit number. They then encrypt these fields by padding with random bits. When a packet reaches a node, the node first decrypts and extracts the random bits from the fields and pads their own random bits. As all the fields of a packet are changed, when a packet moves from node to node, it appears new to the network. This procedure is applicable to all the encrypted fields of all the packets. Encryption/decryption is performed as necessary when a packet moves from node to node.

***RRQSeqNo*:** Route request sequence number *RRQSeqNo* generated by the source uniquely, for the uniqueness of a session.

Ensure Message (EM): This examines the genuineness of the destination. The source generates an EM when it receives the destination's

position. EM = [H_2 (position of destination, time)], where H_2 is the global hash function.

A.2. Route Reply Packet (*RRP)*

E_{C_K} (*RRQSeqNo*)	Sender Temp ID	Receiver Temp ID	*RRPMsg*

Receiver Temp ID: For every session of communication, an intermediate node or the destination generates its Temp ID in the same procedure as the sender Temp ID. Temp ID is the only identification of a node in one session of communication. It is dynamically changeable from session to session. When packets are forwarded, this field is updated by nodes according to their own Temp ID.

A.3. Fail Packet, *(Fail)*

E_{C_K} (*RRQSeqNo*)	Sender Temp ID	Receiver Temp ID	E_{C_K} (NH)

BIBLIOGRAPHY

[1] P. Mohapatra and S. Krishnamurthy, "AD HOC NETWORKS: technologies and protocols", ISBN 0-387-22689-3, *Springer*, pp. xxi-xxiii, 2005.

[2] W. Lou and Y. Fang, "A Survey on Wireless Security in Mobile Ad Hoc Networks: challenges and available solutions", *Book chapter in Ad Hoc Wireless Networking*, Kluwer, May 2003.

[3] Y. Guan, X. Fu, D. Xuan, P. Shenoy, R. Bettati, and W. Zhao, "NetCamo: Camouflaging Network Traffic for QoS-Guaranteed Mission Critical Applications", *IEEE Transactions on Systems, Man, and Cybernetics*, 31(4), pp.253-265, July 2001.

[4] DARPA. "Research Challenges in High Confidence Networking", July 1998.

[5] O. Berg, T. Berg, S. Haavik, J. Hjelmstad, and R. Skaug, "Spread Spectrum in Mobile Communication", *IEEE*, 1998.

[6] S. Jiang, N. Vaidya, and W. Zhao, "Prevent Traffic Analysis in Packet Radio Networks", *Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX II'01), Volume II- Volume 2*, pp.1153-1158, June 2001.

[7] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", *RFC 3561*, July 2003.

[8] D. B. Johnson, D. A. Maltz, and Y. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", *<draft-ietf-manet-dsr-09.txt>*, April 2003.

[9] E. Royer and C-K. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", *IEEE Personal Communications Magazine*, pp. 46-55, April 1999.

[10] Y. Ko and N. Vaidya, "Location-Aided Routing in Mobile Ad Hoc Networks", *Proceedings of the 4th International Conference on Mobile Computing and Networking*, Dallas, USA, pp. 66-75, 1998.

[11] R. Morris and D. De Couto, "Location Proxies and Intermediate Node Forwarding for Practical Geographic Forwarding", *Technical Report MIT-LCS-TR-824, MIT Laboratory for Computer Science*, June 2001.

[12] B. Dahill, B. Levine, E. Royer and C. Shields, "A Secure Routing Protocol for Ad Hoc Networks", *University of Massachusetts Technical Report 01-37*, 2001.

[13] S. Basagni, I. Chlamtac, V. Syrotiuk, and B. Woodward, "A Distance Routing Effect Algorithm for Mobility (DREAM)", *Proceedings of the 4th International Conference on Mobile Computing and Networking*, Dallas, USA, pp.76-84, 1998.

[14] B. Karp and H. Kung, "Greedy Perimeter Stateless Routing for Wireless Networks", *Proceedings of the 6th International Conference on Mobile Computing and Networking*, Boston, USA, pp. 243-254, 2000.

[15] ISO99 ISO IS 15408, 1999, *available at http://www.commoncriteria.org/*

[16] X. Wu and B. Bhargava, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol", *IEEE Transactions on Mobile Computing*, vol. 4, no. 4, pp. 335-348, July/August 2005.

[17] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Secure dynamic distributed routing algorithm for ad hoc wireless networks", *International Conference on Parallel Processing Workshops (ICPPW'03)*, 2003.

[18] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing", *IEEE Journal on Selected Areas in Communications, 16(4)*, pp. 482–494, 1998.

[19] J. Kong and X. Hong, "ANODR: Anonymous on- demand routing with untraceable routes for mobile ad-hoc networks", *Fourth ACM*

International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'03), pp. 291–302, 2003.

[20] B. N. Levine and C. Shields, "Hordes:a multicast based protocol for anonymity", *Journal of Computer Security*, Volume 10, Issue 3, pp. 213 – 240, 2002, ISSN: 0926-227X.

[21] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks", *Technical Report CSD TR # 04-027*, Dept. Computer Sciences, 2004.

[22] Y. Zhang, W. Liu and W. Lou, "Anonymous Communications in Mobile Ad Hoc Networks", In *IEEE Infocom 2005*, Miami, USA, March 13-17, 2005. The *24th Annual Conference Sponsored by IEEE Communications Society, available at http://ece.wpi.edu/~wjlou/publication/INFOCOM05_Zhang.pdf*

[23] Y.C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks", *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, 2003.

[24] A. Abdel-Hafez, A. Miri, and L. Orozco-Barbosa, "Authenticated Secure Communications in Wireless Networks".

[25] M. Ilyas, "The Handbook of Ad Hoc Wireless Networks", CRC Press, Washington D.C., 2003.

[27] Y. Hu, D. Johnson, and A. Perrig. SEAD, "Secure efficient distance vector routing for mobile wireless ad hoc networks", *IEEE Workshop on Mobile Computing Systems and Applications*, June 2002.

[26] L.Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", In *Proceedings of the 2004 Symposium on Network and Distributed Systems Security (NDSS 2004)*, February 2004.

[28] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", In

Proceedings of the SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications, pp. 234–244, August 1994.

[29] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint Relaying: An Efficient Technique for flooding in Mobile Wireless Networks", *Technical Report Research Report RR-3898, Project HIPERCOM*, INRIA, February 2000.

[30] B. Bellur and R. G. Ogier, "A Reliable, Efficient Topology Broadcast Protocol for Dynamic Networks", In *Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'99)*, pages 178–186, March 1999.

[31] D. Boneh, M. Franklin, "Identity Based Encryption from the Weil Pairing", *SIAM Computing*, Vol. 32, No. 3, Extended Abstract in Crypto 2001, pp. 586-615,2003.

[32] P. S. L. M. Berreto, H. Y. Kim and M. Scott, "Efficient algorithms for pairing-based cryptosystems", *Advances in Cryptology - Crypto'2002, LNCS 2442, Springer-Verlag (2002)*, pp.354-368, 2002.

[33] S. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate Pairing", *Algorithm Number Theory Symposium - ANTS V, LNCS 2369, Springer- Verlag (2002)*, pp. 324-337, 2002.

[34] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", *Advances in Cryptology – CRYPTO'01, Lecture Notes in Comput Sci. 2139 (2001)*, pp.213-229, 2001.

[35] D. Boneh, B. Lynn and H. Shachum, "Short signatures from the Weil pairing", *Advances in cryptology –ASIACRYPT'01, Lecture Notes in Comput Sci. 2248 (2001)*, pp.514-532, 2001.

[36] A. Joux and K. nguyen, "Separating decision Diffie-Hellman from Diffie-Hellman in Cryptographic groups", *Cryptology ePrint Archive, Report 2001/03, available at http://eprint.iacr.org/2001/03/.*

[37] R. Dutta, R. Barua and P.Sarkar, "Pairing-Based Cryptographic Protocols: A survey", *Cryptology ePrint Archive, Report 2004/064, available at http://eprint.iacr.org/2004/064*

[38] Y. Ko and N. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks", *Proceedings of the Fourth International Conference on Mobile Computing and Networking (MobiCom'98)*, pp. 66–75, October 1998.

[39] Y. Hu, A. Perrig, and David B. Johnson, Ariadne, "A Secure On-Demand Routing Protocol for Ad Hoc Networks", *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, pp. 12–23, September 2002.

[40] M. G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols", *Proceedings of the ACM Workshop on Wireless Security (WiSe 2002)*, September 2002.

[41] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields and E. B. Royer, "A Secure Routing Protocol for Ad hoc Networks", In *Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP '02)*, November 2002.

[42] C. Castelluccia and G. Montenegro, "Protecting AODV against Impersonation attacks", *Mobile Computing and Communications Review*, pp.108-109 Volume 6, Number 3.

[43] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad Hoc Networks", *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, January 2002.

[44] Y. Xue, B. Li and K. Nahrstedt, "A Scalable Location Management Scheme in Mobile Ad-Hoc Networks", *Proceedings of the 26th IEEE Annual Conference on Local Computer Networks (LCN 2001)*, Tampa, Florida, pp. 102-111, Nov 2001.

[45] X. Wu, "VDPS: Virtual Home Region based Distributed Position Service in Mobile Ad Hoc Networks", *Proc of ICDCS*, 2005.

[46] R. L. Rivest, "The MD5 Message Digest Algorithm", *Internet RFC 1321, April 1992.*

[47] NIST: FIPS 180-1, Secure hash standard, US Department of Commerce, Washing D.C., April, 1995.

[48] Technical Report on the *IEEE 802.11 Protocol*

[49] J.-F. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems", *Proceedings of PET 01*, Vol. 2009, LNCS, Springer-Verlag, pp. 10-29, 2001.

[50] Y. Zhang, "Security in Mobile Ad-hoc networks", *Ad hoc Networks technologies and protocols*, Edited by P Mohapatra and S. Krishnamurthy, Springer, ISBN 0-387-22689-3, pp. 249-268, 2005

[51] S. Carter and A. Yasinasc, "Secure Position Aided Ad hoc Routing Protocol", *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02)*, pp. 329-334, Nov. 4-6, 2002.

[52] H. Y-Chun, A. Perrig, and D.B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols", *WiSe '03: Proceedings of the 2003 ACM workshop on Wireless security*, San Diego, California, USA, ISBN: 1581137699, pp.30-40, September 19, 2003.

[53] "The Tate Pairing", *Available at http://www.computing.dcu.ie/~mike/tate.html*

[54] B. Bhargava and L. Lilien, "Private and Trusted Collaborations," *Proc. Secure. Knowledge Management (SKM): A Workshop*, Amherst, NY, Sept. 2004.

[55] "Quantities of information", *available at http://en.wikipedia.org/wiki/Quantities_of_information*

[56] A. Pfitzmann and M. Kohntopp, “Anonymity, unobservability and pseudonymity- a proposal for terminology”, In *H. Federrah, editor, Designing Privacy Enhancing Technologies: Proceedings of the International Workshop on the Design Issues in Anonymity and Observability*, pp. 1-9, Springer-Verlag, LNCS 2009, July 2000.

[57] C. Diaz, S. Seys, J. Claessens and B. Prenneel, “Towards measuring anonymity”, In *Roger Dingledine and Paul Syverson, editors, Proceedings of the Privacy Enhancing Technologies Workshop (PET 2002), Springer-Verlag, LNCS 2482*, April, 2002.

[58] A. Serjantov and G. Danezis, “Towards an information theoretic metric for anonymity”, In *Roger Dingledine and Paul Syverson, editors, Proceedings of the Privacy Enhancing Technologies Workshop (PET 2002), Springer-Verlag, LNCS 2482*, April, 2002.

PUBLICATIONS

Reviewed Journal Papers

[J1] **S.M.M. Rahman**, A. Inomata, M. Mambo and E. Okamoto, "Anonymous On-Demand Position-based Routing in Mobile Ad-hoc Networks", ***IPSJ*** *(Information Processing Society of Japan)* ***Journal***, Japan, ISSN 0387-5806, Vol. 47, Number 8, pp. 2396-2408, August **2006**.
Online: IPSJ Digital Courier, ISSN 1349-7456, Vol. 2, pp.524-536, 9th August **2006**.

[J2] M.L. Rahman, S. Rafique, M.I. Jabiullah and **S.M.M. Rahman**, "Hash Function Generation for Encryption-free Message Authentication", *Dhaka University Journal of Science*, University of Dhaka, Bangladesh, ISSN 1022-2502, vol. 54, N0. 1, pp.71-73, January **2006**.

[J3] M. I. Jabiullah, **S.M.M. Rahman**, M.L. Rahman and M. A. Hossain, "Pseudorandom Bit String Generation for Secure Electronic Transactions", *Nuclear Science and Applications*, Bangladesh Atomic Energy Commission, Dhaka, Bangladesh, ISSN 1016-197X, Vol. 12, Number 1, 2. pp. 59-61, December **2003**.

[J4] M.I. Jabiullah, M. Rahman, **S.M.M. Rahman** and M.L. Rahman "Encryption with Randomly Chosen Base Conversion and Special Symbols", *Nuclear Science and Applications*, Bangladesh Atomic

Energy Commission, Dhaka, Bangladesh, ISSN 1016-197X, Vol. 12, Number 1, 2. pp. 53-57, December **2003**.

[J5] **S. M. M. Rahman**, M. I. Jabiullah and M. L. Rahman, "Session Key Generation for Message Authentication using Conventional Encryption Techniques", *Journal of Electrical Engineering*, The Institute of Engineers, Bangladesh (JEE–IEB), ISSN 0379 – 4318, Vol. EE 29, No. 2, December 2001, & Vol . EE 30, No. 1, Reg. No . 13/76, pp. 8-12, June **2002**.

[J6] M.S. Islam, **S.M.M. Rahman**, S.M. Masum, S. Parveen, and S. Rafique, "DWDM Technology: Implementation on A Unidirectional System Through Algorithmic Approach", *Journal of Electrical Engineering*, The Institution of Engineers, Bangladesh (JEE–IEB), ISSN 0379-4318, Vol. EE 29, No. 2, December 2001 & Vol. EE 30, No. 1, Reg. No. 13/76, pp. 13-17, June **2002**.

Reviewed International Conference Proceedings

[C1] **S.M.M. Rahman**, A. Inomata, T. Okamoto, M. Mambo and E. Okamoto, "Anonymous Secure Communication in Wireless Mobile Ad-hoc Networks", Pre-proceedings of the First *International Conference on Ubiquitous Convergence Technology (ICUCT2006)*, pp.131-140, Jeju, **Korea**, *Lecture Notes in Computer Science **LNCS** (to appear),* © ***Springer-Verlag***, December 5-6, **2006**. (*Acceptance rate: 5%*)

[C2] **S.M.M. Rahman**, A. Inomata, M. Mambo and E. Okamoto, "An Anonymous On-Demand Position-based Routing in Mobile Ad Hoc Networks", *Proceedings of The 2006 Symposium on Applications & the Internet (SAINT-2006)*, Mesa/Phoenix, Arizona, **USA**, **IEEE** Computer Society Order Number P2508, Library of Congress Number 2005937742, ISBN 0-7695-2508-3, pp. 300-306, January 23-27, **2006**. (*Acceptance rate: 30%*)

[C3] A. Inomata, **S.M.M Rahman**, T. Okamoto, and E. Okamoto, "A Novel Mail Filtering Method Against Phishing", *CD Proceedings 2005 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM '05)*, Victoria BC, **Canada**, **IEEE** Catalog Number: 05CH37690C, ISBN: 0-7803-9196-9, pp. 221-224, August 24-26, **2005**.

[C4] S.M. Masum, **S.M.M. Rahman**, M. Ali, and M.S.I. Khan, "On the Design of Segmented Display for Bengali Digits", *Proceedings of the 8th International Conference on Computer and Information Technology (ICCIT 2005)*, Islamic University of Technology, Gazipur 1704, **Bangladesh**, ISBN 984–32–2873–1, pp. 1120 – 1123, December 28–30, **2005**.

[C5] **S.M.M. Rahma**n and E. Okamoto, "A Quantum Sorting Technique", *Proceedings of the 7th International Conference on Computer and Information Technology (ICCIT 2004)*, Brac University, Dhaka, **Bangladesh**, ISBN 984-32-1836-1, pp. 32-35, December 26–28, **2004**. (Acceptance rate: 24.89%).

[C6] **S.M.M. Rahman**, S.M. Masum, M.S.I. Khan, M.S. Alam, and M.I. Hasan, "A New Message Digest Function for Message Authentication", *CD Proceedings of the 4th WSEAS International Conference on Information Science and Applications (ISA 2004)* , Miami, Florida, **USA**, ISBN 960–8052–97–1, April 21–23, **2004**.

[C7] **S.M.M. Rahman,** S.M. Masum, M.S.I. Khan, M.L. Rahman, and E. Okamoto, "Message Digest and Integrity Checking using Hash Function", *Proceedings of the 6th International Conference on Computer and Information Technology (ICCIT 2003),* Jahangirnagar University, Dhaka 1342, **Bangladesh**, ISBN 984–584–005–1, Vol. I, pp. 136–138, December 19–21, **2003**.

[C8] M. I. Jabiullah, A.A. Shamim, **S.M.M. Rahman,** M.L. Rahman "Session Key Generation using Conventional Encryption Techniques", *Proceedings of the 6th International Conference on Computer & Information Technology (ICCIT 2003),* Jahangirnagar University, Dhaka 1342, **Bangladesh**. ISBN 984 -584- 005-1, pp. 200–205, December 19-21, **2003**.

[C9] M.S. Islam, **S.M.M. Rahman**, S.M. Masum, S. Parveen, and S. Rafique, "DWDM Technology: Implementation on A Unidirectional System through Algorithmic Approach", *Proceedings of the 4th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2003)*, Chengdu, Sichuan, **China**, **IEEE** Catalog No. 03EX684, ISBN 0–7803–7840–7, Library of Congress 2003101499, pp. 282 – 285, August 27–29, **2003**.

[C10] S.M. Masum, M.S.I. Khan, **S.M.M. Rahman,** and M. Ali, "Designing 10–Segment Display for Bangla Digits", *Proceedings of the 3rd International Conference on Electrical, Electronics and Computer Engineering (ICEECE 2003)*, Stamford University Bangladesh, Dhaka 1217, Bangladesh, ISBN 984–31–1528–7, pp. 161–164, December 22–24, **2003**.

[C11] M. I. Jabiullah, **S. M. M. Rahman** and M. L. Rahman, "Session Key Generation For Message Authentication Using Conventional Encryption Techniques", *Proceedings of the 3rd International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT' 02)*, Kanazawa Bunka Hall, Kanazawa, **Japan**, ISBN 4-9900330-2-73-6, pp. 278–282, September 3-6, **2002**.

[C12] M. I. Jabiullah, **S.M.M. Rahman**, M.L. Rahman and M. A. Hossain, "Secure Pseudorandom Bit Generation For Cryptographic Applications", *Proceedings of the 4th International Conference on Computer and Information Technology (ICCIT 2001)*, University of Dhaka, Dhaka, **Bangladesh**. ISBN 984-32-015-2, pp. 275 – 277, December 28–29, **2001**.

Symposium Proceedings

[S1] **S.M.M.Rahman,** A. Inomata, T. Okamoto, M. Mambo, and E. Okamoto, "Anonymous Communication in Wireless Mobile Ad-hoc Networks", *Proceedings of the Computer Security Symposium 2006 (CSS2006)*, Kyoto, Japan, Information Processing Society of Japan, IPSJ Symposium Series Vol. 2006, No.11, ISSN 1344-0640, pp. 375-380, October 25-27, **2006**.

[S2] A. Inomata, **S.M.M Rahman**, T. Okamoto, and E. Okamoto, "Propose of Mail Filter Method Against Phishing", *Proceedings of the 2005 Symposium on Cryptography and Information Security (SCIS 2005)*, Kobe, Japan, pp. 193-198, January 25th - 28th, **2005**.

[S3] **S.M.M. Rahman** and E. Okamoto, "A Partial Image Encryption Based on the Center Point and Chaotic System", *Proceedings of the Computer Security Symposium 2004 (CSS2004)*, Hokkaido University, Hokkaido, Japan, Information Processing Society of Japan, IPSJ, Symposium Series Vol. 2004, No.11, ISSN 1344-0640, pp. 673-677, October 20-22, **2004**.