Islamic University – Gaza
Deanery of Higher Studies
Faculty of Engineering
Computer Engineering Department

Secure Zone Routing Protocol in Ad-Hoc Networks

Hanan M. M. Abu-Thuraia

Supervisor

Prof. Ibrahim S. I. Abuhaiba

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Engineering

1431H (2010)

ACKNOWLEDGMENT

It is my pleasure to express my gratitude to all the people who contributed, in whatever manner, to the success of this work.

First and foremost, I would like to express my sincere gratitude to ALLAH for blessing me with the potential and ability to work on this master thesis. Then I would like to thank Prof. Ibrahim Abuhaiba who has rendered continuous and encouraging guidance throughout the entire thesis period.

Thanks to my husband, and my parents who unremittingly supported me during my years of study.

Finally I'd like to thank my friends and well-wishers for helping me by careful reviews of my work and inspiriting suggestion.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

AODV	:	Ad-hoc On-demand Distance Vector Routing
BRP	:	Bordercast Resolution Protocol
CA	:	Certification Authority
CBR	:	Constant Bit Rate
DoS	:	Denial of Service
DSA	:	Digital Signature Algorithm
DSDV	:	Destination Sequenced Distance Vector Routing
DSN	:	Destination Sequence Number
DSR	:	Dynamic Source Routing
DT	:	Distance Table
ECA	:	Elliptic Curve Algorithm
GPS	:	Global Position System
IARP	:	IntrA-zone Routing Protocol
IERP	:	IntEr-zone Routing Protocol
KDC	:	Key Distribution Center
LAN	:	Local Area Network
LCT	:	Link Cost Table
MAC	:	Medium Access Control
MANETs	:	Mobile Ad-hoc NETwork
NDP	:	Neighbor Discovery Protocol
PDA	:	Personal Digital Assistant
PKC	:	Public-Key Cryptography
RERR	:	Route Error Packet
MRL	:	Message Retransmission List
RREP	:	Route Replay Packet
RREQ	:	Route Request Packet
RSA	:	Rivest – Shamir-Adleman

RT : Routing Table

SKC : Symmetric-Key Cryptography

SZRP : Secure Zone Routing Protocol

TTL : Time To Live

TTP : Trusted Third Party

UI : Unique Identifier

WRP : Wireless Routing Protocol

ZRP : Zone Routing Protocol

Secure Zone Routing Protocol in Ad-Hoc Networks

Hanan M. M. Abu-Thuraia

ABSTRACT

A mobile ad-hoc network is a collection of mobile nodes connected together over a wireless medium without any fixed infrastructure. Currently, ad-hoc networks are gaining popularity for their attractive features and applications. Security in such networks is an essential component that safeguards the proper functioning of the network and underlying protocols. However, the inconsistency between some properties of the nodes nature such as high mobility, energy-constraint, no central administration, and the security requirements of its allied application make achieving secure routing a nontrivial task.

Traditionally, routing protocols for wireless ad-hoc networks assume a non-adversarial environment and a cooperative network setting. In practice, there may be malicious nodes that attempt to disrupt the network communication by launching attacks on the network or the routing protocol itself.

This thesis is a contribution in the field of security analysis on mobile ad-hoc networks, and security requirements of applications. Limitations of the mobile nodes have been studied in order to design a secure routing protocol that thwarts different kinds of attacks. Our approach is based on the Zone Routing Protocol (ZRP); the most popular hybrid routing protocol. The importance of the proposed solution lies in the fact that it ensures security as needed by providing a comprehensive architecture of secure zone routing protocol based on efficient key management, secure neighbor discovery, secure routing packets, detection of malicious nodes, and preventing these nodes from destroying the network. In order to fulfill these objectives, both efficient key management and secure neighbor mechanisms have been designed to be performed prior to the functioning of the protocol.

To validate the proposed solution, we use the network simulator NS-2 to test the performance of secure protocol and compare it with the conventional zone routing protocol over different number of factors that affect the network. Our results evidently show that our secure version paragons the conventional protocol in the packet delivery ratio while it has a tolerable increase in the routing overhead and average delay. Also, security analysis proves in details that the proposed protocol is robust enough to thwart all classes of ad-hoc attacks.

***Keywords*:** Ad-hoc networks, secure routing, secure neighbor discovery, digital signature, zone routing protocol.

بروتوكول التوجيه المنطقي الآمن في الشبكات العشوائية

حنان محمد مجدي أبوثريا

الملخص

شبكات المحمول العشوائية هي عبارة عن مجموعة من النقاط المتصلة معا من خلال وسائط لاسلكية دون الاعتماد على أي بنية تحتية ثابتة. حالياً، تكتسب هذه الشبكات اللاسلكية العشوائية رواجاً واسعاً لمميزاتها الجذابة وتطبيقاتها المختلفة. ويعتبر تحقيق الأمن في هذه الشبكات من العناصر الأساسية لضمان حسن سير العمل في الشبكة والبروتوكولات التابعة لها. ومع ذلك، فإن التناقض بين خصائص أجهزة هذه الشبكات مثل سرعة التنقل، محدودية الطاقة المتوفرة، غياب الإدارة المركزية، والمتطلبات الأمنية للتطبيقات المختلفة يجعل تحقيق الأمن في بروتوكولات التوجيه أمراً ليس بالهين.

تقليدياً، معظم بروتوكولات التوجيه للشبكات اللاسلكية العشوائية تفترض بيئة خالية من النقاط المعادية، وأن جميع النقاط هي نقاط متعاونة، ولكن في الواقع قد يكون هناك نقاط معادية تحاول تعطيل عمل الشبكة من خلال شن هجمات على شبكة الاتصال عامةً أو على بروتوكولات التوجيه بشكل خاص.

تعتبر أطروحة الماجستير هذه مساهمة لتحليل الهجمات التي تواجه بروتوكولات التوجيه في الشبكات اللاسلكية العشوائية، ومتطلبات الأمن من قبل التطبيقات المختلفة. وقد تم أخذ القصور في أجهزة الشبكات اللاسلكية بعين الاعتبار من أجل تصميم بروتوكول توجيهي آمن له القدرة على إحباط جميع أنواع الهجمات. ويعتمد النظام المقترح على بروتوكول التوجيه المنطقي والذي يعد أشهر البروتوكولات الهجينة، وتكمن أهميه الحل المقترح في حقيقة أنه يضمن الأمن من خلال توفير بنية شاملة تعتمد على إدارة فعالة لإنشاء وتوزيع المفاتيح الآمنة، الاكتشاف الآمن للنقاط المجاورة، أمن حزم التوجيه، وإمكانية اكتشاف النقاط المعادية ومنعها من إحباط عمل الشبكة. هذا ومن أجل تحقيق جميع الأهداف فإن كلاً من الإدارة الفعالة لإنشاء وتوزيع المفاتيح الآمنة، والاكتشاف الآمن للنقاط المجاورة صممت لتعمل قبل عمل البروتوكول الرئيسي.

وللتحقق من صحة الحل المقترح، تم تنفيذ عمليات محاكاة لقياس أداء البروتوكول المقدم ومقارنته مع البروتوكول التقليدي باستخدام عدد من العوامل المختلفة التي تؤثر على أداء الشبكة. وقد أوضحت النتائج أن الإصدار الآمن يضاهي بروتوكول التوجيه المنطقي التقليدي في نسبة الحزم المستلمة، في حين أن هناك زيادة مقبولة في الأحمال الزائدة فيما يتعلق بحجم البيانات المرسلة وعدد الحزم، وكذلك في متوسط التأخير. كذلك فإن تحليل الأمن يثبت بالتفصيل أن البروتوكول المقترح هو قوي بما يكفي لإحباط جميع أنواع الهجمات.

الكلمات المفتاحية **:**الشبكات العشوائية، التوجيه الآمن، الاكتشاف الآمن للنقاط المجاورة، التوقيع الرقمي، بروتوكول التوجيه المنطقي.

Chapter 1

INTRODUCTION

1.1 Motivations

Most computers communicate with each other by using wired networks. This approach is well suited for stationary computers, but it is not appropriate for mobile devices. Mobile devices can use wireless networks almost anywhere and anytime by using one or more wireless network technologies such as mobile ad-hoc networks. An ad-hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure [8]. These mobile nodes communicate directly via wireless links within their radio range while these which are far apart depend on other nodes to relay messages. Mobile networks were of primary interest in military communications and disaster relief because of their “infrastructure-less" nature. However, over the past decade these networks gained popularity in the form of personal-area networks and civilian networks.

One of the most demanding and challenging aspects of ad-hoc networks is the routing issue [1]. Routing can be defined as the process of finding a path from the source to the destination to deliver packets to the destination nodes while the nodes in the network are moving freely. Thus, each node acts as a router as well as an end-node to relay or receive packets in the network [46]. Routing is a challenging task in mobile ad-hoc networks because of many reasons such as node mobility, lack of predefined infrastructure, peer-to-peer mode of communication and limited radio range. Currently, there does not exist any standard for a routing protocol for ad-hoc networks, instead this is a work in progress [17].

Secure routing is also a vital factor for mobile ad-hoc networks because of the sensitive applications of these networks. However, achieving security goals, such as confidentiality, authentication, integrity, availability, and access control in these networks is a challenging task. In general, a mobile ad-hoc network is particularly vulnerable to attacks due to its fundamental characteristics of open medium, dynamic topology, distributed cooperation, constrained capability, and absence of central authorities [9].

1.2 Wireless Networks

Wireless communication between mobile users is becoming more popular than ever before. This has been fed by the growing technological advances in laptop computers and wireless data communication devices, such as wireless modems and wireless LANs. Conceptually, two different kinds of wireless networks exist, a reliable infrastructure wireless network such as cellular network, and infrastructure-less network or more commonly Mobile Ad-hoc Networks (MANETs).

1.2.1. Cellular Networks

In this kind of networks, a wireless network is built on the top of a "wired" network. The wireless nodes are connected to the wired network and are able to act as bridges. The major issue in such a network is related to the concept of handoff, where one base station tries to hand off a connection to another seamlessly, without any noticeable delay or packet loss. A practical problem in networks based on cellular infrastructure is that it is limited to places where there exists such a cellular network infrastructure [17].

1.2.2. MANETs Networks

The term ad-hoc translates to "improvised" or "not organized" and refers to the dynamic nature of such a network. MANETs consist of a set of handset devices usually mobile and wire free. Typical devices of MANETs are Personal Digital Assistants PDAs, laptops, cell phones, and notebooks that exchange data with each other. These devices can freely move in the network, leave or join the network at any time, and finally, the network disappears when the last device leaves the network. They are self configured and have the ability to operate without any infrastructure in place except for the participating mobile devices [17].

1.2.3. Characteristic of MANETs Networks

MANETs are *temporary* networks because they are formed to fulfill a special purpose and cease to exist after fulfilling this purpose. Mobile devices might arbitrarily join or leave the network at any time, thus MANETs have *a dynamic infrastructure*. Most mobile devices use radio or infrared frequencies for their communications which leads to a very *limited transmission range*. Usually the transmission range is increased by

using multi-hop routing paths, where all or some nodes within MANETs are expected to be able to route data packets for other nodes in the network who want to reach nodes beyond their own transmission range. In that case, a device sends its packets to its neighbor devices. Those neighbor nodes then forward the packets to their neighbors until the packets reach their destination. The most distinguishing property of MANETs is that the networks are *self-organized*. All network interactions have to be executable in absence of a Trusted Third Party (TTP). Hence, in contrast to wired networks, ad-hoc networks do not rely on a fixed infrastructure and the accessibility of a TTP. The self-organizing property is unique to ad-hoc networks and makes implementing security protocols a very challenging task. Other characteristics of MANETs are the *constrained network devices*. The constraints of MANETs' devices are a small CPU, small memory, small bandwidth, weak physical protection, and limited battery power. In most ad-hoc networks all devices have similar constraints [52].

1.2.4. MANETs Applications

MANETs do not rely on any pre-established infrastructure and can therefore be deployed in places lacking traditional infrastructure. This is useful in disaster recovery situations and places with non-existing or damaged communication infrastructure and where rapid deployment of a communication network is needed. MANETs are also used at business meetings and conferences to confidentially exchange data, at the library to access the Internet with a laptop, and at hospitals to transfer confidential data from a medical device to a doctor’s PDA. Many more applications exist already or are imaginable in the near future as it is expected that ad-hoc networking will be more intensively used for different applications such as digital battlefield communications, movable base-stations, and range extension for cellular telephone [1].

1.2.5. Security Goals in MANETs

The special properties of ad-hoc networks enable all the neat features in such networks have to offer, but at the same time, those properties make implementing security protocols very difficult to achieve. There are four main security problems that need to be dealt with in ad-hoc networks: (1) the authentication of devices that wish to talk to each other, (2) the secure key establishment of a session key among authenticated

devices, (3) the secure routing in multi-hop networks; and (4) the secure data transmission [1].

1.2.6. Difficulties and Challenges

The attractive features of MANETs are the major causes for rapid popularity in various applications. However, these features act as burdens on achieving the required security goals; some of these features and their effects are discussed below:

The dependence on radio transmission, as the most mean of communication, makes eavesdropping on a node easier than in wired networks. Since intermediate nodes no longer belong to a trusted infrastructure, and may be eavesdroppers as well, consequent end-to-end encryption is mandatory.

Next, as all nodes in MANETs cooperate in order to discover the network topology and forward packets, denial of service attacks on the routing function are very easy to mount. Nodes may create stale or wrong routes, creating black holes or routing loops.

Furthermore, in MANETs there exists a strong motivation for non-participation in the routing system. Both the routing system and the forwarding of foreign packets consume a node's battery power, CPU time, and bandwidth, which are restricted in mobile devices.

Finally, MANETs are highly dynamic in nature. Node joins and departures are performed without any prediction. Moreover, network topology is always changed in such a network. Therefore any static security mechanism will not be applicable in MANETs. In other words, security primitives must be dynamically adjusted to cope with the network which is, of course, a daunting task [14].

1.3 Aim of this Thesis

The main goal of this master thesis is to present a secure zone routing protocol by providing an implementation of four mechanisms. To achieve this goal, key management, and secure neighbor detections are presented as pre-requirements to provide a trusted environment. Then a secure routing protocol is proposed to provide the integrity and authenticity of the packets follow in the existing Zone Routing Protocol (ZRP) [6]. Our work is based on performing two security mechanisms; digital signature and hash function, to assure the achievement of security goals and countering

the existing attacks. Finally, the proposed work relies on detection of malicious nodes mechanism to prevent misbehaving nodes from disrupting the network.

1.4 Methods Used

To accomplish the proposed solution, the following methods have been used in sequence:

- Study the basic principles of mobile ad-hoc networks.
- Review of the existing routing protocols, especially ZRP.
- Identifying the major attacks in routing and the major points of vulnerability.
- Study the protocols proposed to secure routing protocols, and identify their weakness.
- Design of a set of related security mechanisms.
- Redesign zone routing protocol using the suggested mechanisms.
- Demonstrate the validity of the proposed protocol to defend against different kinds of attacks threatening mobile networks.

1.5 Our Approach

The new secure zone routing protocol has been implemented in C language and network simulator NS-2 is used for its evaluation and comparison with the non-secure version of the protocol. Our evaluation metrics include; packet delivery ratio, routing overhead in packets, routing overhead in bytes, and average end-to-end latency. The comparisons are performed under different circumstances such as mobility pattern, transmission rate, network size, and zone radius.

In addition, we introduce an analytical method to demonstrate how the new protocol can counter all types of attacks that threat mobile ad-hoc networks. Using a numerical approach, we show that breaking the security of our secure protocol and obtaining the secret keys are out of reach.

1.6 Organization of this Thesis

The rest of the thesis is organized as follows. Chapter 2 presents a brief review of well known routing protocols for mobile ad-hoc networks with a detailed description of ZRP, and considers categories of the lately proposed solutions to secure both reactive and

proactive routing protocols. A survey of security goals, possible attacks that threaten ad-hoc networks, and cryptograph techniques are discussed in chapter 3. Chapter 4 presents a formal description of our design of secure zone routing protocol with required parameters, assumptions, and all prerequisite mechanisms needed to make this comprehensive work. Validation of security functionalities of proposed secure protocol are provided in chapter 5. Chapter 6 discusses in details the simulation methodology, lists the parameters, and analyzes the results obtained by evaluating the secure protocol under different scenarios. The report ends with conclusions in chapter 7 which summarizes this thesis and gives some hints for future work on this subject.

Chapter 2

ROUTING IN AD-HOC MOBILE NETWORK

Routing in ad-hoc networks is the process of selecting paths in a network by which a packet travels from a source to a destination in a timely manner [46]; thus each node acts as a router as well as an end-node to relay or receive packets in the network. Routing is a daunting task in MANETs because of the characteristics of the network related to node mobility, self deployment, hop-to-hop communication and constrained resources. Several protocols [2-6] have been proposed in the literature for routing in ad-hoc networks that are excellent in terms of efficiency. At the core, all these routing protocols try to find an optimal route from the source to the destination, assuming that all nodes in the network are trusted and cooperative. One of the most interesting aspects of these investigations concerns whether or not nodes in an ad-hoc network should keep track of routes to all possible destinations, or instead keep track of only those destinations of immediate interest because a route established by a source may not exist after a short interval of time. Depending on how nodes establish and maintain a route to the required destination, routing protocols for ad-hoc networks broadly fall into proactive, reactive, and hybrid categories. Till today, there is no standard routing protocol for mobile ad-hoc networks [52].

2.1 Proactive Routing Protocols

Proactive approach is a table-driven protocol, where each node attempts to maintain consistent up-to-date routing information to every other node in the network by maintaining one or more tables. Routing information is stored and maintained before the actual transmission begins. From application perspective, it has the advantage of minimum initial delay as the desired route is already established. However, these proactive protocols cause substantial signaling traffic and power consumption problems, and mostly can result in higher overhead due to the route maintenance and frequent route updates. Destination Sequenced Distance Vector Routing (DSDV) and Wireless Routing Protocol (WRP) are two examples of this category.

2.1.1 Destination Sequenced Distance Vector Routing

In DSDV [5], each node acts as a specialized router, advertises its view of the interconnection topology with other mobile nodes within the network. Routing table is maintained at each node, where all the possible destinations and the number of hops to them in the network are recorded. Each entry in the routing table consists of the destination ID, the next hop ID, a hop count, and a sequence number for that destination. The sequence number helps nodes maintain a fresh route to the destination, find out stale routes, and avoid routing loops. To cope with frequently changing network topology, nodes periodically broadcast routing table updates throughout the network. To decrease the overhead produced, each node has the ability to send two types of updates – full dump and incremental –that contain all entries in its routing table or only the entries that have been changed since the last update. Changes to the routing table entries are performed only if the sequence number of the destination in the update packet is higher than the one in its routing table.

2.1.2 Wireless Routing Protocol

WRP uses an enhanced version of DSDV protocol; it introduces mechanisms which reduce route loops and ensure reliable message exchange. While DSDV maintains only one topology table, WRP uses a set of tables to maintain more accurate information. These tables are: Distance Table (DT), Routing Table (RT), Link Cost Table (LCT), and a Message Retransmission List (MRL). Nodes periodically exchange routing tables via update messages, or whenever the link state table changes. The MRL maintains a list of neighbors which are yet to acknowledge an update message, so they can be retransmitted if necessary. When an update message is received, a node updates its distance table and reassesses the best route paths. It also carries out a consistency check with its neighbors, to help eliminate loops and speed up convergence. WRP requires large memory storage and resources in maintaining its tables; so it is not suitable for large mobile ad-hoc networks.

2.2 Reactive Routing Protocols

Reactive routing protocols are demand-driven where routing information is acquired only when it is actually needed. Establishing a new route involves a route discovery phase consisting of a route request (flooding) and a route replay once a route is found. Reactive routing protocols may often use far less bandwidth for maintaining the route tables at each node, but the latency will drastically increase. Moreover, the reactive route search procedure may involve significant control traffic due to global flooding. This may make pure reactive routing less suitable for real-time traffic. Ad-hoc on demand Distance Vector Protocol (AODV) and Dynamic Source Routing (DSR) are two examples of this type.

2.2.1 Ad-hoc On demand Distance Vector Protocol

In AODV protocol [4], a source broadcasts a Route Request packet (RREQ) to its neighbors when it has a packet to send to some destination and does not currently have a route to that destination. Each node maintains a monotonically increasing counter called broadcast ID, where broadcast ID along with the IP address of the node uniquely identifies the RREQ in the entire network. The source also uses a Destination Sequence Number (DSN) to determine an up-to-date path to the destination. A node updates its path information only if the DSN of the current packet received is greater than the last DSN stored at the node. Each intermediate node increments the hop count field in RREQ by one and broadcasts this RREQ until it reaches the destination or a node that has a higher DSN. Multiple replies (Route Replies - RREPs) may be generated and transmitted along the reverse path. Each intermediate node increments the hop count in RREP and updates its routing table if the RREP has a higher DSN or a shorter hop count. This continues until the RREP gets back to the source node. When a node detects a path-break, it drops the packet for the destination, generates a route error packet (RERR) and sends it to the source which tries to re-establish a path to the destination. One of the disadvantages of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number.

2.2.2 Dynamic Source Routing

DSR [3] was one of the first reactive routing protocols. It uses RREQ, RREP, and RERR packets to establish and maintain path to the destination. However, unlike AODV, these packets accumulate a list of node IDs along the path from the source to the destination, and vice versa. This list is embedded in the packet header when transmitting the data.

Each node learns routes to other nodes when it initiates a RREQ to a particular destination or when it lies on an active path to that destination. In addition to these, a node may also learn a route by overhearing transmissions along the routes of which it is not a part.

2.3 Hybrid Routing Protocols

Hybrid protocols combine the advantages of both purely proactive and purely reactive routing protocols for optimal performance. They separate a node's local neighborhood from the global topology. Zone routing protocol is one of such hybrid protocols that takes the advantage of proactive discovery within a node's neighborhood, and uses a reactive protocol for communication between these neighborhoods based on the fact that the most communication takes place between nodes close to each other. Changes in the topology are most important in the vicinity of a node - the addition or removal of a node on the other side of the network has only limited impact on the local neighborhoods [52, 65].

2.4 Zone Routing Protocol - ZRP

ZRP [6] aims to address excess bandwidth and long route request delay of proactive and reactive routing protocols. It combines the advantages of these approaches by maintaining an up-to-date topological map centered on each node. The separation of a node's local neighborhood from the global topology of the entire network allows for applying different approaches, and thus taking advantage of each technique's features for a given situation. These local neighborhoods are called *zones*; each node may be within multiple overlapping zones, and each zone may be of a different size. The size of a zone is not determined by geographical measurement, as one might expect, but is given by a radius of length ρ, where ρ is the number of hops to the perimeter of the

zone. Thus, a zone includes all nodes whose distance from the center node is at most ρ hops. An example of a routing zone with radius two is shown in figure 2.1, where the routing zone of S includes the nodes A–K, but not L.

The nodes of a zone are divided into peripheral nodes whose minimum distance to the center is exactly equal to zone radius, gray nodes, and interior nodes whose minimum distance to the center is less than zone radius, white nodes.

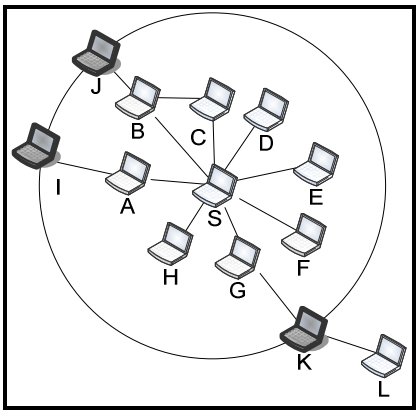


Figure 2.1: Routing zone with radius ρ = 2

The nodes A–H are interior nodes, the nodes I-K are peripheral nodes, and the node L is outside the routing zone. Note that node J can be reached by two paths, one with length 2 through node B, and one with length 3 hops through node C and B. The node is however within the zone, since the shortest path is less than or equal to the zone radius.

2.4.1 ZRP Architecture

The architecture of ZRP is illustrated in figure 2.2; the IntrA-zone Routing Protocol (IARP) [66] is considered as the locally proactive routing component which is used by a node to communicate with the interior nodes of its zone and as well is limited by the zones radius. Since the local neighborhood of a node may rapidly be changing, and these changes in the local topology are likely to have a bigger impact on a node's routing behavior than a change on the other end of the network, the IARP is a proactive table-driven protocol. Each node continuously needs to update the routing information in order to determine the peripheral nodes as well as maintain a map of which nodes can be reached locally. The IARP allows for local route optimization through the removal of redundant routes and the shortening of routes if a route with fewer hops has been detected, as well as bypassing link-failures through multiple hops. IARP is very efficient where routes to local destinations are immediately available.

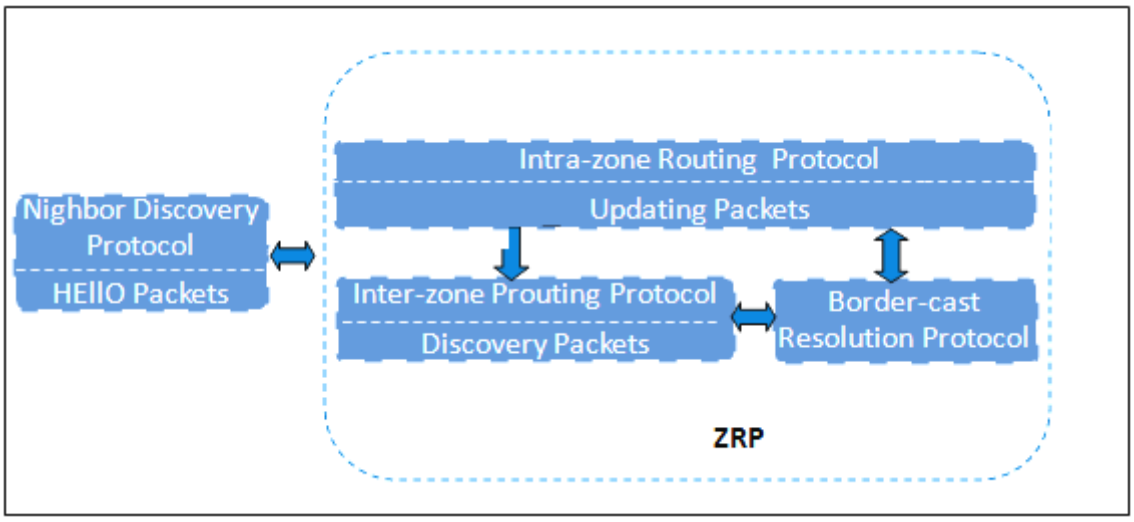


Figure 2.2: Architecture of ZRP

The globally reactive routing component is named IntEr-zone Routing Protocol (IERP) [67] which offers enhanced route discovery and route maintenance services. The IERP needs to be able to take advantage of the local connectivity provided by IARP, as well as change the way route discovery is handled. Instead of flooding a route request to all nodes, it uses the Bordercast Resolution Protocol (BRP) [68] to only transmit route requests to peripheral nodes.

Border-cast resolution protocol is used to direct the route requests initiated by the global reactive IERP to the peripheral nodes, thus removing redundant queries and maximizing efficiency. In doing so, it utilizes the map provided by the local proactive IARP to construct a bordercast tree. Unlike IARP and IERP, it is not so much a routing protocol, as it is packet delivery service.

Finally, each node uses Neighbor Discovery Protocol (NDP) [50] in order to construct a routing zone and to determine the peripheral nodes and link failures. Such protocol typically relies on the transmission of "HELLO" beacons by each node at regular intervals. If a node receives a response to such a message, it may note that it has a direct point-to-point connection with this neighbor. The NDP is free to select nodes on various criteria, such as signal strength or frequency/delay of beacons, etc. Once the local routing information has been collected, the node periodically broadcasts discovery messages in order to keep its map of neighbors up to date.

2.4.2 Routing in ZRP

A node that has a packet to send first checks whether the destination is within its local zone using information provided by IARP. In that case, the packet can be routed proactively. Reactive routing is used if the destination is outside the zone. The reactive routing process is divided into two phases: the route request phase and the route reply phase. In the route request, the source sends a route request packet to its peripheral nodes using BRP. If the receiver of a route request packet knows the destination, it responds by sending a route reply back to the source. Otherwise, it continues the process by border-casting the packet. The reply is sent by any node that can provide a route to the destination. To be able to send the reply back to the source node, routing information must be accumulated when the request is sent through the network. The information is recorded either in the route request packet, or as next-hop addresses in the nodes along the path. When the packet reaches the destination, the sequence of addresses is reversed and copied to the route reply packet [6].

2.4.3 Query-Control Mechanisms

In bordercasting technique, route request packets are only sent to the peripheral nodes, and thus only on the corresponding links, which makes it more efficient than flooding. However, each node may forward route requests several times due to overlapping zones, which results in more traffic than in flooding. The excess traffic is a result from queries returning to covered zones instead of covered nodes as in traditional flooding.
In order to solve this problem, ZRP uses query control mechanisms, query detection, early termination and random query-processing delay. In query detection mechanism, it is possible to detect quires relayed by other nodes in the same zone to prevent them from reappearing in the covered zone. In addition, a node can prevent a route request from entering already covered regions by using early termination. This mechanism combines information obtained through query detection with the knowledge of the local topology to prune branches leading to peripheral nodes inside covered regions. A node can also prune a peripheral node if it has already relayed a query to that node. Finally, random query processing delay can be employed to reduce the probability of receiving the same request from several nodes. Each bordercasting node waits a random time before the construction of the bordercast tree and the early termination. During this

time, the waiting node can detect queries from other bordercasting nodes and prune the bordercast tree [6].

2.5 Secure Routing Protocols

Routing protocol security has become a significant issue. The open and dynamic nature of ad-hoc networks leads to many opportunities for attacks to occur given the heavy reliance on cooperative nodes and trust required for them to function correctly.

In this section, we give an overview of existing approaches that attempt to provide security to MANETs routing protocols. The existing approaches are described and compared with respect to their security objectives, the applied security mechanisms, and performance criteria. These approaches are ARAN [12], ARIADNE [9], SEAD [8], and SAODV [10] which have the same purpose of securing MANETs routing protocols. However, they are based on different protocols and use special mechanisms which will be considered shortly.

2.5.1 Authenticated Routing for Ad-hoc Networks

ARAN is based on AODV [4], but provides authentication of route discovery, setup, and maintenance. It consists of a preliminary certification process followed by a route instantiation process that detects and protects against malicious actions by third parties and peers in one particular ad-hoc environment where no network infrastructure is pre deployed; however, it expects a small amount of prior security coordination. ARAN introduces authentication, message integrity, and non-repudiation using pre-determined cryptographic certificates.

ARAN requires the use of a trusted certificate server whose public key is known by all valid nodes. Before entering the ad-hoc network, each node requests a certificate from the server. A nonce and timestamp together are used to ensure freshness when used in a network with a limited clock skew. Compared to basic AODV, ARAN prevents a number of attacks, including spoofing of route signaling messages and alteration of routing messages. Also, replay attacks are prevented by a nonce and timestamp. The authors in [12] show that ARAN presents a good performance, equivalent to AODV, in discovering and maintaining routes. Besides its problems in handling scalability with

the number of nodes, it has performance costs in terms of packets overhead, higher latency, and processing time

2.5.2 A Secure On Demand Routing Protocol

In [9], a model for the types of attacks on ad-hoc networks is given and a new secure routing protocol based on DSR protocol is proposed. The proposed protocol relies on three approaches to provide authenticity with low computational and communication overhead: 1) TESLA (Timed Efficient Stream Loss- tolerant Authentication) [20, 21] that requires loose time synchronization for authentication of nodes on the routing path, 2) digital signature, and 3) message authentication code.

The main objective of ARIADNE is to provide authentication and integrity of DSR signaling messages, i.e., routing discovery and route maintenance. It has the advantage of preventing unauthorized nodes from sending route error packets because it is required that each message is authenticated also.

ARIADNE protects DSR from a number of attacks, including routing loops, black/grey holes, and replay. Regarding performance, it is noting that every intermediate node increases the length of the signaling messages which results in large signaling packets for long routes. Also, key disclosure increases the end-to-end delay of a route discovery process. Both issues negatively impact the packet delivery ratio, in particular for highly mobile scenarios. Finally, it requires clock synchronization, which is considered to be an unrealistic requirement for ad-hoc networks.

2.5.3 Secure Efficient Distance Vector Routing

In [8], authors provide a secure ad-hoc routing protocol based on DSDV protocol in a bidirectional network, but the main ideas can be applied in other distance vector protocols. The main objective is to protect MANETs against multiple uncoordinated attackers creating incorrect routing state in any other node. In order to be deployed in an environment with low computational power and to guard against DoS attacks in which an attacker tries to make other nodes consume excessive bandwidth or processing time, an efficient one-way hash chain is used to authenticate routing information, and a destination sequence number is used to provide replay protection where any attacker cannot create a valid advertisement with larger (better) sequence number that it

received. It can be used with any suitable authentication and key distribution scheme. But finding such a scheme is not straightforward.

Although SEAD outperforms DSDV in terms of packet delivery ratio; it creates more overhead in the network. It cannot prevent the same distance attack where a node can re-advertise the same sequence number and metric [52].

2.5.4 Securing Ad-hoc Routing Protocol

SAODV [10] is a secure extension for AODV. The main objectives of SAODV are integrity, authentication, and non-repudiation of AODV routing information. It uses two mechanisms to secure messages: digital signatures to authenticate the unchangeable fields of messages, and hash chains to secure the hop count information which is the only mutable information in the packets. It has the disadvantage of assuming the existence of a key management sub-system.

SAODV has the same performance characteristics as AODV. However, the known problems of AODV become a greater problem in SAODV. It is well known that AODV increases the packet overhead when the mobility increases. This will even be a bigger problem for SAODV since the processing of each packet requires some extra processing time, due to the usage of cryptography. As in SEAD, the protocol can't prevent the same distance attacks.

2.5.5 Secure Protocols against Specific Attacks

Other researchers proposed to provide a secure ad-hoc routing protocol against specific attacks such as:

Wormholes Attack [22-23]: where an attacker records packets at one location in the network, tunnels them to another location, and retransmits them there into the network. This attack can be prevented by packet leashes [22], or identify malicious nodes by statistically analyzing the information collected by multi-path routing [23].

Rushing Attack: which results in denial-of-service when used against all on-demand ad-hoc network routing protocols. The authors in [25] provide three mechanisms to defend important class of protocols against the rushing attack. These include secure neighbor detection, secure route delegation, and randomized route request forwarding. Because

the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks.

Many security issues have not been tackled in most of pervious works such as:

- Most proposed protocols assume bidirectional channel, but it is probably that one node can successfully send packets to the other while no communication is possible in the reverse direction. This refers to the difference of the antenna, propagation patterns or sources of interference around the two nodes.
- Secure routing protocols assume an existence of central trust authority for implementing traditional cryptographic algorithms. However, these assumptions don't hold in ad-hoc networks.
- Hybrid protocols aren’t considered. Some researchers define securing hybrid protocols as future works [8, 9].

Chapter 3

SECURITY IN AD-HOC NETWORKS

3.1 Security Goals

Security is a vital factor for MANETs due to its sensitive applications. However, the characteristics of MANETs pose both challenges and opportunities in achieving security goals that need to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation.

Confidentiality: The goal of confidentiality is to keep the information sent unreadable to unauthorized users or nodes. MANETs use an open medium; so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data, or use directional antennas.

Authentication: The goal of authentication is to ensure that a communicating entity is communicating with another legitimate entity. Without authentication an attacker can impersonate an authenticated node and thus gain control over the entire network. In wired networks and infrastructure-based wireless networks, it is possible to implement a central authority at a point such as a router, base station, or access point. But there is no central authority in MANETs, and it is much more difficult to authenticate an entity.

Integrity: The goal of integrity is to be able to keep the message sent from being illegally altered or destroyed in the transmission. When the data is sent through the wireless medium, the data can be modified or deleted by malicious attackers. The integrity can be achieved by hash functions in order to be certain that changes to a transferred message are done by authorized entities through authorized mechanisms.

Non-repudiation: The goal of non-repudiation is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by him. By producing a signature for the message, the entity cannot later deny the message. It is particularly useful for detecting a compromised node.

Availability: The goal of availability is to keep the network service or resources available to authorized entities even though there is potential problem in the system. Lack of availability ensures denial of service (DoS) attacks.

Access control: The goal of access control is to prevent unauthorized use of network services and system resources. In general, access control is the most commonly thought of service in both network communications and individual computer systems [57].

3.2 Types of Attacks

Security always implies the identification of potential attacks, threats, and vulnerabilities of a certain system. A useful mean of classifying security attacks is in terms of passive attacks and active attacks.

3.2.1 Passive Attacks

In a passive attack, the attacker does not disrupt the operation of a routing protocol or affect system resources but only attempts to discover valuable information by listening to the routing traffic. The major advantage for the attacker in passive attacks is that in a wireless environment the attack is usually impossible to detect. This also makes defending against such attacks difficult. Furthermore, routing information can reveal relationships between nodes or disclose their IP addresses. If a route to a particular node is requested more often than to other nodes, the attacker might expect that the node is important for the functioning of the network, and disabling it could bring the entire network down [31].

3.2.2 Active Attacks

To perform an active attack the attacker must be able to inject arbitrary packets into the network. The goal involves some modification of the data stream or the creation of a false stream or just to disable the network. A major difference in comparison with passive attacks is that an active attack can sometimes be detected. This makes active attacks a less inviting option for most attackers.

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delay caused by them. If the detection has a deterrent effect, it may also contribute to prevention [31].

3.3 Possible Attacks on Routing Protocols

In this section, we classify attacks that are targeting the network later by attacking the routing protocols; attackers can absorb network traffic, inject themselves into the path between the source and destination, and thus control the network traffic flow.

3.3.1 Attacks Using Modification

Malicious nodes can cause redirection of network traffic and DoS attacks by altering control message fields or by forwarding routing messages with falsified value. Below are the details of several attacks that can occur if particular fields of routing messages are altered or falsified.

- **Modification to Sequence Number:**

As mentioned previously, DSN is used to determine up-to-date routes to destination which is monotonically increased. An attacker may divert traffic through itself by advertising a greater DSN than the authentic value [1].

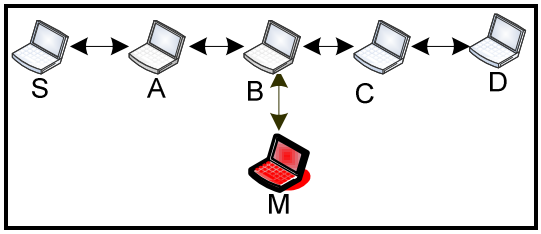


Figure 3.1: An example of modification attack

For example, node S in figure 3.1 sends a RREQ with DSN. A malicious node M receives it and sends a RREP reply with greater destination sequence number to B. Thus M can redirect all traffic to itself. When B receives the valid RREP, it discards the packet as it has a lower DSN. All subsequent traffic destined for D that travels through B will be directed toward M, so a denial of service attack is launched.

- **Lengthen/Shorten the Route**

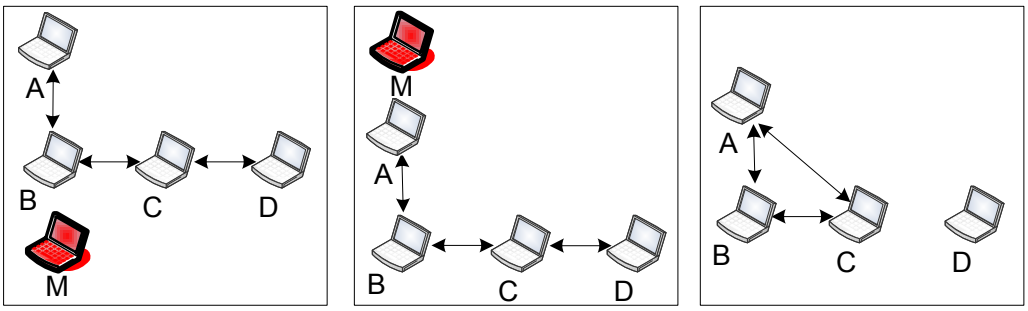
An attacker can receive the packet and add itself to the node list of the route or remove a node from the node list so that it can be included or excluded from the route. Another reason of lengthening the route is to make the route less attractive and hence it is avoided.

3.3.2 Attacks Using Impersonation

Nodes can misrepresent their identity in the network by altering their MAC or IP address in outgoing packets. The following example illustrates how an impersonation attack can degrade the performance of ZRP.

- **Forming Loops**

For the network topology shown in figure 3.2, M starts attacking by changing its MAC address to impersonate A, and sends RREP packet to B that holds the path to D with a greater DSN. B will change its route to the destination D to go through A. Then, the attacker M impersonate the node B as in figure 3.2(b), and sends a RREP to C containing B as a next hop, so C will change its route to D via B. At this point as in figure 3.2 (c), a loop is formed and no packet will reach the destination D.



(a) (b) (c)

Figure 3.2: An example of impersonating attack

3.3.3 Attacks Using Fabrication

The vulnerability is that routing attacks can be launched by sending false route error messages. A malicious node in figure 3.3 sends routing message to B spoofing node C, indicating a link error to D. B will delete its routing table entry to D, and broadcast routing packets to all neighbors to delete D entry from their routing tables. In this case, the malicious node succeeds in preventing communication to D from all nodes.

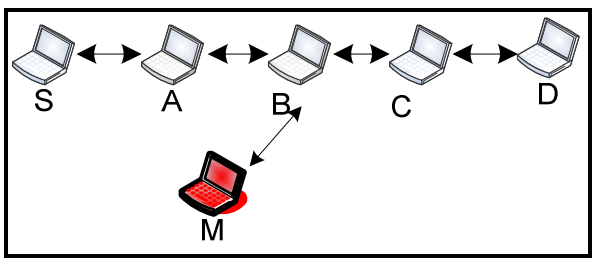


Figure 3.3: An example of fabrication attack

3.3.4 Other Advanced Attacks

Advanced and sophisticated attacks such as black-hole, worm-hole, and rushing attacks have been identified in separated research [22-25]. Below, we will describe most of these harmful attacks:

- **Black-hole attacks**

Black-hole attack is a type of denial-of-service attack accomplished by dropping packets. The attacker attracts all packets by falsely claiming a fresh route to the destination, and then absorbs them without forwarding them to the destination. This technique can be launched to all packets for a particular network destination or a randomly selected portion of the packets, which is called "Gray-hole attack".

- **Worm-hole attacks**

In this type of attack [22-24], a malicious node exploits that a direct (tunneling) link is faster than a general hop-by-hop propagation. An attacker records packets at one location in the network, tunnels them to another location via a low-latency link, and retransmits them there into the network.
Wormhole attack is difficult to detect since it can be launched without compromising any node or the integrity and authenticity of communication.

- **Rushing attacks**

Hu et al. [25] introduce rushing attacks that act as an effective denial-of-service attack against all ad-hoc routing protocols. An attacker exploits the mechanism of suppressing duplicate route requests by quickly forwarding route request packets to its neighbors' nodes. When non-attacking requests arrive later at these nodes, they will discard those legitimate requests. This means that these nodes will not forward any route request packets from this route discovery phase.

3.4 Cryptographic Mechanisms

Attackers may require a variety of countermeasures to defend against their work; one of a primary method of protecting valuable electronic information is cryptography. In the past, cryptography referred only to the encryption and decryption of the message using

secret keys. Today, it has three different mechanisms: symmetric-key encipherment, asymmetric key encipherment, and Hashing [57].

3.4.1 Symmetric-Key Encipherment

In symmetric key encipherment, the sender - Alice uses an encryption algorithm to encrypt the original message (plaintext) using a secret key shared with the recipient as illustrated in figure 3.4 [57]. The generated massage (cipher-text) is transmitted through insecure channel. The recipient –Bob decrypts the cipher-text using the same shared key to obtain the plaintext.

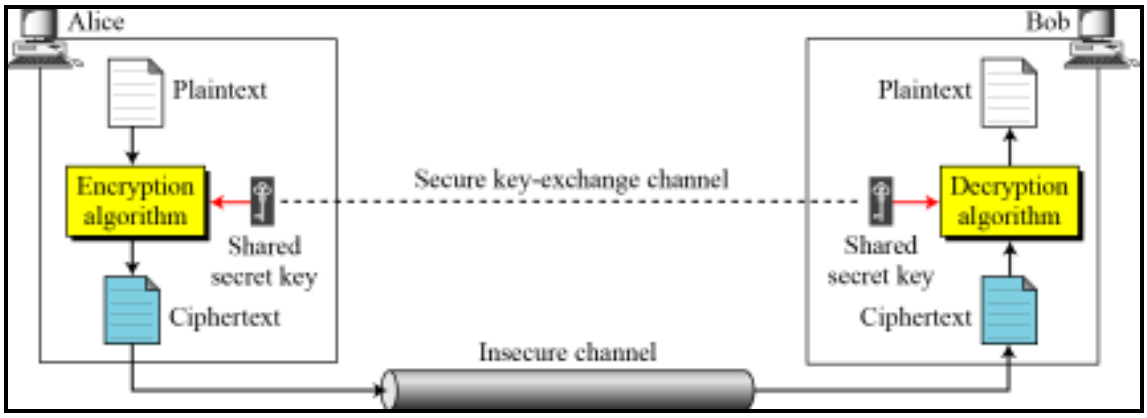


Figure 3.4: General idea of symmetric key encipherment

Symmetric-key is a very efficient form of encryption, but it needs two requirements for secure use of it. The first is to use a strong encryption/decryption algorithm, while the other is to provide a secure fashion to transfer the secret key between the two entities.

3.4.2 Asymmetric-Key Encipherment

Asymmetric key encipherment or public-key encipherment is shown in figure 3.5 [57]. In this scheme, there are two keys instead of one; public key and private key. Each user generates a pair of keys to be used for encryption and decryption of messages. Depending on the application, the sender uses either the sender's private key or the receiver's public key, or both, to perform some types of cryptographic function. One of the most well-known applications of this mechanism is digital signature.

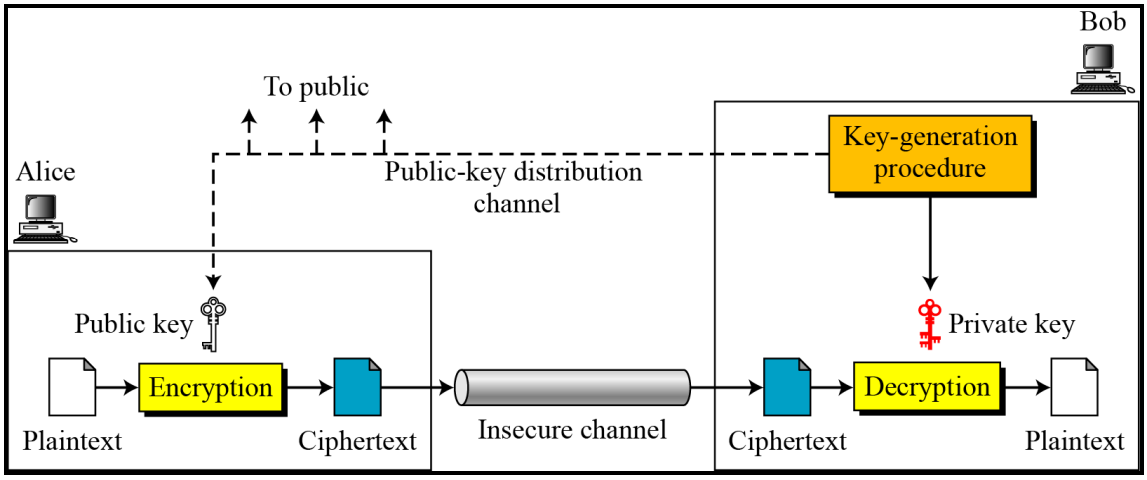


Figure 3.5: General idea of asymmetric key encipherment

With this approach, private keys are generated locally by each participant and therefore don't need key distribution center that is considered as the most difficult problem associated with symmetric encryption.

3.4.3 Hashing

In hashing, a fixed-length message digest is created out of a variable-length message. The hash value is appended to the message at the source at a time when the message is assumed to be known or correct. The receiver authenticates that message by re-computing the hash value. Because the hash function itself is not considered to be secret, some means is required to protect the hash value. Message Digest (MD) and Secure Hash Algorithms (SHA) are two types of hash functions used in cryptography. Both functions satisfy the following properties:

- ***Collision resistance***

An adversary should not be able to find two distinct messages M and M′ such that H(M) = H(M′).

- ***First Preimage Resistance:***

An adversary given a target image D should not be able to find a preimage M such that H(M) = D. One reason why this property is important is that on most computer systems user passwords are stored as the cryptographic hash of the password instead of just the plaintext password. Thus an adversary who gains access to the password file cannot use

it to then gain access to the system, unless it is able to invert target message digests of the hash function.

- ***Second Preimage Resistance:***

An adversary given a message M should not be able to find another message M′ such that M = M′ and H(M′) = H(M). This property is implied by collision resistance.

- **Secure Hash Algorithm (SHA-1)**

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely-used security applications and protocols such as IPsec[70]. SHA-1 takes a multiple blocks message with a maximum length of $(2^{64} - 1)$ bits and produces a 160-bit digest which is designed so that it should be computationally expensive to find a text which matches a given hash. Each block is 512 bits in length. SHA-1 is based on preprocessing and computation phases. In preprocessing phase, the message M is padded to ensure that it is a multiple of 512 bits. Then, the padded message is parsed into N 512-bit blocks, and a hash value, $H^{(0)}$, consisting of five 32-bit words is initialized. After the preprocessing is completed, each message block, is processed to produce 160-bit message digest.

3.4.4 Digital Signature

A digital signature is a mathematical scheme for demonstrating the authenticity, data integrity, and non-repudiation of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. The recipient can also prove that the message is indeed signed by the sender if he claims to have sent the message. Different schemes of digital signature have been widely used. They rely either on integer factorization as (Rivest - Shamir - Adleman) RSA, discrete logarithm as Digital Signature Algorithm – DSA which has been criticized from the time it was published or elliptic curve discrete logarithm as Elliptic Curve Algorithm - ECA.

Although ECA offers even smaller key sizes and have always been significantly faster than signing with RSA, verification with RSA was faster, and ECA is mathematically more subtle; difficult to pick a particular curve for a particular application [61].

- **RSA Digital Signature Scheme**

RSA is the most common pubic key algorithm, named for its inventors. It is based on one-way modular exponentiation functions. It uses a large number n in addition to two exponents, e and d, where e is public while d is private. The algorithm involves three steps: key generation, signing, and verifying. In key generation process, a node creates its public/private keys (e,d,n), announces the pair(e,n) as a public key while the value of d is kept as private.

The signing and verifying processes are shown in figure 3.6 [57]. The sender creates a signature (S) out of the message (M) using its private key, sends both the message and the signature to the receipt. Once the receiver receives the message and the signature, it uses the sender's public key to create a copy of the message M'. It compares M with M', accepts the message if the two values are congruent.

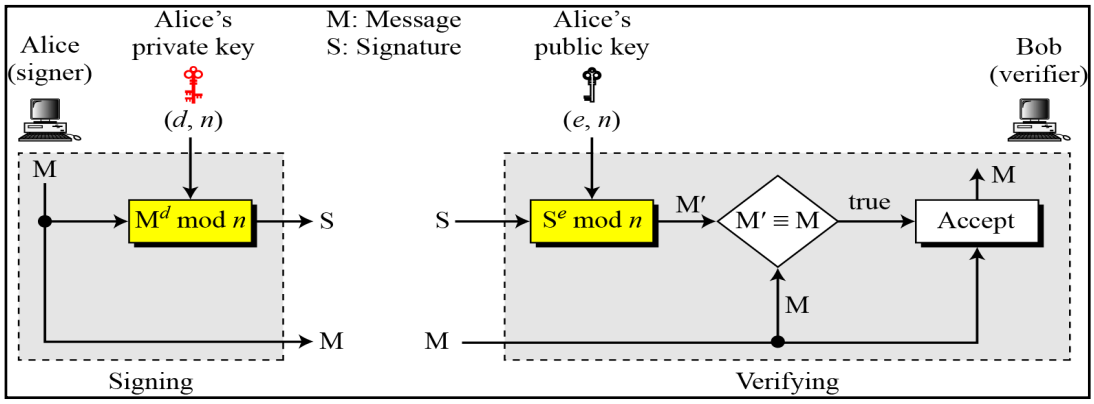


Figure 3.6: RSA digital signature scheme

Chapter 4

METHODOLOGY OF THE PROPOSED SZRP

The attractive features of ad-hoc networks such as open medium, dynamic topology, absence of central authorities, and distributed cooperation hold the promise of revolutionizing the ad-hoc networks across a range of civil, scientific, military and industrial applications.

However, these characteristics make ad-hoc networks vulnerable to different types of attacks and make implementing security in ad-hoc network a challenging task. The main security problems that need to be dealt with in ad-hoc networks include: the identity authentication of devices that wish to talk to each other, the secure key establishment of keys among authenticated devices, the secure routing in multi-hop networks, and the secure transfer of data [1]. This means that the receiver should be able to confirm that the identity of the source or the sender (i.e., one hop previous node) is indeed who or what it claims to be. It also means that the receiver should be able to verify that the content of a message has not been altered either maliciously or accidentally in transit. Our proposed work is based on securing one of the most popular hybrid protocols: zone routing protocol. The basic operation of ZRP is discussed in section 2.4. We use a multi-hop ad-hoc network consisting of n nodes. Each node is responsible for relaying messages from source S to destination D. Each node has its private/public key, and other nodes can use its public key in verification processes.

4.1 Our Contribution

We present an implementation of Secure Zone Routing Protocol based on the conventional ZRP (figure 2.2) that isn't secure and doesn't consider security requirements. We modify it by using four stages as shown in figure 4.1; first, we use an efficient key management mechanism that is considered as a prerequisite for any security mechanism. Then, we provide a secure neighbor detection scheme that relies on neighbor discovery, time and location based protocols [50, 62]. Securing routing packets is considered as the third stage which depends on verifying the authenticity of the sender and the integrity of the packets received. Finally, detection of malicious

nodes mechanism is used to identify misbehaving nodes and isolate them using blacklist. Once these goals are achieved, providing confidentiality of transferred data becomes an easy task which can be implemented using any cryptography system.

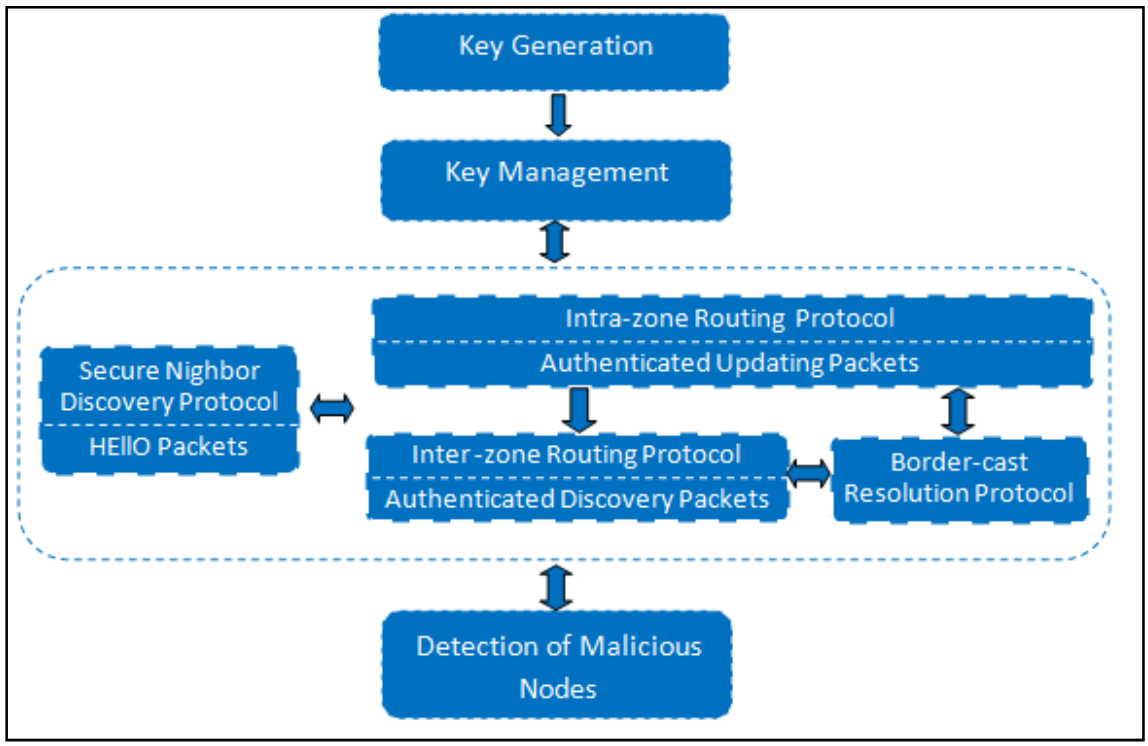


Figure 4.1: Architecture of SZRP

4.2 Design Goals

For our design to be suitable for ad-hoc networks, the following design goals should be met:

- Few computational steps to reserve the limited power of all ad-hoc devices since too many computational steps will drain the battery.
- Balanced protocol, which means that all nodes should perform approximately the same number of heavily computations.
- Few packets flows with small size since large packets are spitted into several packets to match the available communication bandwidth where sending many packets contradicts with the previous design goal.
- Restricted number of heavy computations, such as modular exponentiations, to save battery power although the processors of most ad-hoc devices are becoming more powerful and can perform these computations.

4.3 Assumptions

Network Assumption

- Although the physical layer of wireless network is often vulnerable to denial of service attacks such as jamming. Many researchers have proposed mechanisms to resist physical jamming such as spread spectrum [64], so this type of attack is beyond the scope of this thesis.
- We assume that the network links are either unidirectional or bidirectional; that is, if node A is able to transmit to some node B, node B doesn't necessarily have the ability to transmit to node A. Most recent researches that have been proposed to secure routing protocols assume bidirectional links [8-12]; although it isn't always true.

Node Assumption

- We assume that all nodes have loosely synchronized clock, and have the ability to define its location in order to perform neighbor authentication. Accurate time synchronization and location can be maintained with Global Position System - GPS[63].
- We don't assume trusted hardware. Secure routing with trusted hardware is much simple since node compromise is assumed to be impossible.
- We assume that nodes in the ad-hoc networks are resource constrained. Thus, in IERP, we use efficient symmetric cryptography in hop-to-hop transfer, rather than relying on expensive asymmetric cryptographic operations. Especially on CPU-limited devices, symmetric cryptographic operations (such as hash functions) are three to four orders of magnitude faster than asymmetric cryptographic operation [8, 13, and 22].
- We assume that each node has its private/public key pair, and has the ability to know the public keys of all other nodes.
- We base our design on the absence of public key infrastructure, or any trusted distribution center. Most previous works on secure MANETs routing protocols rely on them for the secrecy and authenticity of keys stored in nodes. However, this requirement of a central trust authority and pre-configuration is neither

practical nor feasible in MANETs due to the self deployment, dynamic topology, and the lack of central authorities.

4.4 System Notations

We use the following notations to describe our model. They are used by the protocols, known to the protocol designer and to the adversary.

A, B	: Principals, such as communication nodes.
K_A^-	: The public key of node A.
K_A^+	: The private key of node A.
R	: The neighbor discovery range.
T_t	: The time at which the packet is transmitted.
T_r	: The time at which the packet is received.
L_A	: The location of node A obtained using GPS.
Δt	: The expected delay depending on the wireless channel.
v	: Signal propagation speed.
$RSA_K\ (M)$	: The computation of the digital signature of a message M with the key K using RSA algorithm
$Verify_K\ (M,S)$	: The process of verifying the signature S of the message M using the key k
H[M]	: The computation of the hash value of message M using SHA-1.

4.5 Key Generation

Key generation is the process of calculating new key pairs for security purposes. In our design, this includes generation of public/private key pair for digital signature. The generation process is performed when the node is created (***bootstrapping phase***) using the steps shown in Algorithm 4.1 [57] where the size of n, d, and e are 512, 128 and 17 bits, respectively.

Algorithm 4.1: Key_Generation

{

Select two large prime numbers p and q such that p≠q

$n \leftarrow p \times q$

$\Phi(n) \leftarrow (p\text{-}1)\times(q\text{-}1)$

Select e such that $1 \leq e \leq \Phi(n)$ and e is co-prime to $\Phi(n)$

$d \leftarrow e^{-1} \bmod \Phi(n)$

$K_A^- \leftarrow (e,n)$

$K_A^+ \leftarrow d$

Return $K_A^- and K_A^+$

}

After key generation, the node keeps its private key and announces the public key in neighbor advertisement message in response to neighbor solicitations message and after verification of its neighbors as we will discuss shortly.

4.6 Key Management

Many efforts have been devoted to securing peer communications in wireless ad-hoc networks, and most of them are based on either symmetric-key cryptography (SKC) or public-key cryptography (PKC) systems; many of them are found to be inadequate for wireless ad-hoc networks, either due to severe communication or computing constraints, or due to the lack of infrastructure support in such networks.

One issue, key management, is of the greatest interest, since it is a prerequisite for any security procedures of publicly-known cryptographic algorithms. For example, in SKC, shared keys or pre-shared secrets should be arranged for involved nodes before they can communicate; in PKC, senders should obtain the public-key of receivers and verify it with trusted third-parties.

For communication in MANETs, nodes need to identify other nodes of their interest. Therefore, mobile nodes can be identified by their own identity of spatial and temporal invariance. For example, nodes propose their identity when joining MANETs systems. Nodes should be assisted with additional security procedures to ensure the confidentiality, integrity, and authenticity of their information exchange with intended nodes. Without the help of a trusted key distribution center (KDC), or a trusted

certification authority (CA) or any preexisting communication and security infrastructures, nodes may have to deal with unknown relaying nodes without the pre-established trust worthiness, and hence become vulnerable to various passive and active attacks.

To overcome this weakness, we base our design on the concept of identity-based key management which serves as a prerequisite for various security procedures.

The basic idea is to use an identifier that has a strong cryptographic binding with the public key, and components of the mobile node in the same manner that is suggested for MIPv6 in [69]. We will call this identifier, Unique Identifier (UI). This identifier should be owned and used exclusively by the created node.

An address (64-bits) that satisfies properties of required UI is obtained using steps shown in algorithm 4.2 which are described as follows:

- The most 32-bits refer to the MAC address of the node.
- The least 32-bits refer to certain processing on the public key generated by the node at bootstrapping phase, these bits are extracted by 1) Compute the hash value of the public key using SHA-1, 2) Divide the hash value into four parts each of 32-bits, and 3) Perform an XOR operation on the divided hash values and the location of the node (L used as an evidence).

Algorithm 4.2: Generate Unique Identifier

{

L ←Location of the node using GPS system

Digest ←H[$\boldsymbol{K_A^-}$].

Break the digest into four chunks (Do-D3)

UI← Concatenate (*MAC, (*$D_o \otimes D_1 \otimes D_2 \otimes D_3 \otimes$ L*)*

Return UI

}

This unique identifier that is composed of the concatenation of the IP address and the hash value of the public key is secure because an attacker can't produce a new pair of keys that has the same hash value due to second pre-image resistance of one-way hash function, or discover the private key for the given public key.

After obtaining the UI, key management mechanism is performed as follows:

- The mobile node sends binding update message MSG1 containing the UI described above with a nonce to its corresponding node.
- The corresponding node replies with MSG2 containing the same nonce produced by the mobile node.
- When receiving MSG2, the mobile node verifies that the nonce is the same as what it was sent in MSG1. It sends MSG3 that contains its public key and the evidence used to generate the UI. This message is signed by the private key of the mobile node.
- When the corresponding node receives MSG3, it verifies the signature using the included public key, and verifies that this public key and the evidence produce the same least 32-bits of the UI. Once the message passes the two verifications, it concludes that the mobile node owns this address and the public key. The corresponding node stores the address and the key of the mobile node to be used in further mechanisms.

The key management mechanism proposed is believed to be efficient since nodes can safely trust the corresponding nodes when they claim ownership of that identifier. It also will not increase the complexity of the network because 1) Not all nodes need to use the mechanisms, only those nodes that wish to perform binding updates, 2) Not all nodes needs to verify MSG3, only those nodes that want to accept the binding update, and 3) Messages are exchanged directly between the mobile node and its neighbors and are not routed to other nodes.

4.7 Secure Neighbor Discovery

In wireless networks, each node needs to know its neighbors to make routing decisions; it stores neighbor information in its routing table that contains the address of the neighbor, and the link state. In MANETs, nodes use neighbor discovery protocol to discover surrounding nodes they can directly communicate with across the wireless channel with signal propagation speed by considering the location or round trip information. Two different nodes, A and B, are considered as neighbors and thus can exchange information directly if and only if the Euclidean distance between them |AB| is less than or equal to the neighbor discovery range, R.

The NDP protocol relies on HELLO message exchange. Hello messages are used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that includes all its neighbors. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected [50].

The nodes need a correct view of neighbor information that raises the importance of applying a secure neighbor detection protocol. NDP protocol is widely used; however, it can be easily attacked due to lack of security. A malicious node can easily relay or replay packets deluding other nodes that they are communicated directly. Many methods have been proposed to protect neighbor information in hostile environments [22]. However, these methods can only protect neighbor relation between benign nodes while compromised nodes can easily circumvent them and setup false relations.

In our model, we use a combination of two techniques that rely on time and location based on secure neighbor discovery mechanisms. We based our design on NDP protocol and use the same HELLO message to decrease the number of message flows, and hence the loss of power. Time based protocol (T-based), requires nodes to transmit authenticated messages containing a time-stamp set at the time of sending. Upon receipt of such a message, a receiver checks its freshness by verifying that the message time-stamp is within a threshold of the receiver's current time. If so, it accepts the message creator as a neighbor. T-based protocols aren't efficient in all cases. For example, they lead to impossibly results if the adversary node has the ability to relay a packet under the predefined threshold value.

In time and location based protocols (TL-based), a node requires sending authenticated messages containing a time-stamp set at the time of sending, and their own location. Upon receipt of such a message sent from a node B, the receiver A calculates two estimates; the first estimate is based on the difference of its own clock at reception time and the message's time-stamp. The second one is calculated with the help of the location. If the two distance estimates are equal, A accepts B as a neighbor.

The proposed secure NDP protocol consists of three rounds; in the first round the nodes broadcast a HELLO message with its location, the time of sending, and the authentication part $RSA_{K_A^+}(T_A,L_A)$ which indicates that location and the time of sending is authenticated by node A. Authentication process is performed using digital signature

with the private key of node A. when the packet is received in the second round, the receiver computes the distance using the location values stored in the packet and transmission time, then compares the results obtained with the range of transmission as demonstrated in figure 4.2. If the two distance estimates are equal, it verifies the signature. Once the signature is verified, B accepts A as neighbor, signs the packet and replies with beacon acknowledge. Once node A receives the beacon acknowledges it compares the evidence L_A with the transmitted one; if the two values are equal, it verifies the signature of the received packet using B's public key. If verification process is checked correctly, node A accepts B as a neighbor, and updates its entire table by assigning a zero value to the trust level of node B.

A		:	$Signature=RSA_{K_A^+}(T_A,L_A)$
A	→*	:	<*HELLO message, T_A, L_A, Signature* >
B		:	$T \leftarrow (T_A+\Delta t)-Tr$
		:	$D_1 \leftarrow c \times T$
		:	$D_2 \leftarrow \lvert L_A-L_B \rvert$
		:	IIF (D_1=D_2&& D_1<=R)
		:	$V \leftarrow Verify_{K_A^-}((T_A,L_A),Signature)$
		:	*If (V = TRUE)*
		:	Accept A as a neighbor
		:	Else, Reject the packet
B	→A	:	<*ACK, L_A, Signature* >
A		:	$V \leftarrow Verify_{K_B^-}(Signature)$
			Accept B as a neighbor
			Update the neighbor table

Figure 4.2: Three rounds of secure neighbor discovery

* Indicates broadcast address

Here, we assumed that corresponding nodes have accurate time and location information based on synchronize clocks and GPS. Inaccurate time and location information can be easily handled by taking into account an acceptable small difference (e.g. inaccurate parameter) when comparing the estimated values.

4.8 Secure Routing Packets

Once we achieve secure information exchange, we can further secure the underlying routing protocol in wireless ad-hoc networks. Security services in MANETs belong to two kinds of massages: the routing massages and the data messages. Both have a different nature and different security needs. We focus here on securing routing because data messages are point-to-point and can be protected with any point-to-point security system. On the other hand, routing messages are sent to intermediate neighbors, processed, possibly modified, and resent. Moreover, as a result of processing of routing message, a node might modify its routing table. This creates the need for both the end-to-end and the intermediate nodes to be able to authenticate the information contained in the routing messages.

If all routing messages in MANETs are encrypted with a symmetric cryptography, it means that every member wants to participate in the network has to know the common key. This is the best solution for military networks or any trusted-members network where every member should know the common key before joining the network. However, that is not a suitable solution for a conventional MANETs such as meeting room or campus in which members aren't trusted [19]. The best option is to use asymmetric cryptography so that the originator of the route messages signs the message. It would not be needed to encrypt the routing messages because they are not secret. The only requirement is that the nodes will be able to detect forged routing messages. To accomplish this goal we use both digital signature and one-way hash function to attain message authentication, and message integrity as illustrated in algorithm 4.3, and described in more details in the following sections.

Algorithm 4.3: Secure Rotting Packets

```
Input: new routing packet P from source S to destination D.
{
    Signature ←RSA_{K_S^-}(P).
    Select Case (P.type)
    Case 1: IAPR
            If (Signature=P.signature)
                    Update tables.
```

```
                Update the packet according to ZRP procedures.
                Signature ←RSA_{K_D^+}(P).
                Append Signature to the packet P.
                Broadcast the packet to neighbors.
                Return 0
        Else
                Drop the packet
                Detection of Malicious node(S)
                Return 0
        End If
    Break;
    Case 2: IEPR
        Digest ←H[p].
        If (Signature=P.signature && Digest=P.digest)
                Update tables.
                Update the packet according to ZRP procedures.
                Signature ←RSA_{K_D^+}(P).
                Digest ←H[P].
                Append Signature and Digest to the packet P.
                Bordercast the packet to peripheral nodes.
                Return 0
         Else
                Drop the packet
                Detection of Malicious node(S)
                Return 0
        End If
    Break;
End Select
}
```

4.8.1 Secure Intra Zone Routing Protocol

To provide packet authentication and message integrity in IARP, digital signature using RSA is used. The IARP packet format is shown in figure 4.3.

Link Source Address			
Link State Sequence Num		Zone Radius	TTL
RESERVED	RESERVED	Link Destination Count	
Link Destination 1 Address			
Link Destination 1 Subnet Mask (Optional)			
RESERVED	Metric Type	Metric Value	
RESERVED	Metric Type	Metric Value	
…….			
Link Destination n Address			
Link Destination n Subnet Mask (Optional)			
RESERVED	Metric Type	Metric Value	
RESERVED	Metric Type	Metric Value	
Signature			

Figure 4.3: Link state IARP packet format

All shaded fields in the packet will be signed using RSA algorithm using the private key of the sender. The signature is stored in the packet before broadcasting it to its neighbors. This signature will provide the authenticity and integrity of the sender and the packet respectively.

- **Secure IARP Scenario**

Each node periodically advertises its link state (current set of neighbors and corresponding lists of link metrics) through its routing zone. The scope of link state update is controlled by the Time-To-Live (TTL) value that is initialized with the zone radius minus one. The source node signs the whole packet using its private key, appends the signature to the packet, and broadcast it to its surrounding neighbors.

Upon receipt of link state update packet, the receiver starts processing the packet if the sender has a high trusted value. Once this is achieved, the receiver creates a copy of the message using the public key of the source already stored in its neighbors' table, and compares the result with the received massage. If the packet passes the verification process, the routing table is recomputed and the packet's TTL value is decremented. The process is repeated as long as the TTL value is greater than zero. The scenario of securing IARP packet is shown in figure 4.4.

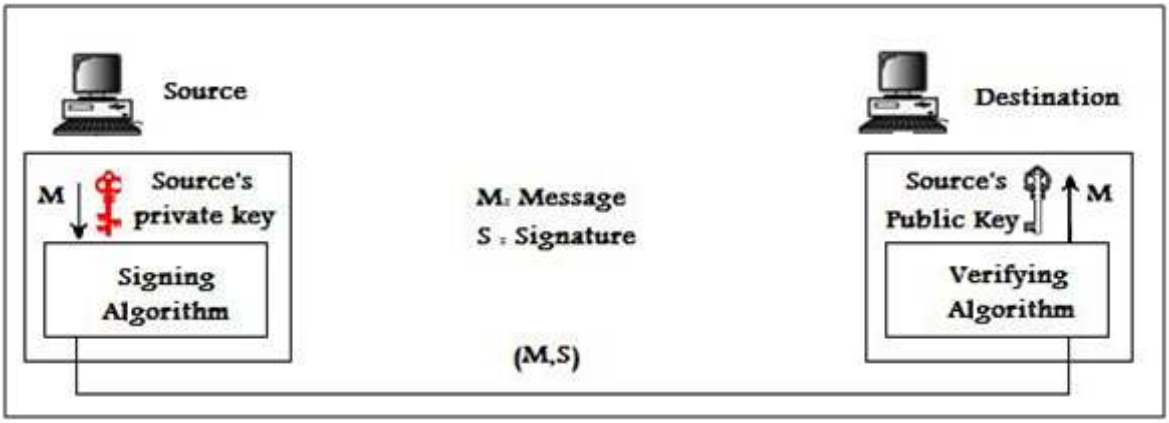


Figure 4.4: Secure IARP scenario

4.8.2 Secure Inter Zone Routing Protocol

To secure IERP packets, we make end-to-end authentication using digital signature of the non-mutable fields of the packets, the dashed fields of the packet as illustrated in figure 4.5, and a one-way hash function to achieve the integrity of mutable fields while the packets are transmitted through intermediate nodes. The information generated by applying the hash function and the digital signature is transmitted within the packet that we will refer to by signature and digest.

Type	Length	Node Ptr	RESERVED
Query ID		RESERVED	
Query/Route Source Address			
Intermediate Node (1) Address			
Intermediate Node (2) Address			

Intermediate Node (n) Address			
Query/Route Destination Address			
Signature			
Digest			

Non-Mutable Fields Mutable Fields

Figure 4.5: IERP packet format

We use the terms IERP digital signature, and IERP hashing to identify the two mechanisms that are used to secure IERP packets. More details about the functionality of these mechanisms follow.

- **IERP Digital Signature**

Digital signature using RSA is used to protect the integrity of the non-mutable fields of the packet using the private key of the initiator. The signature is stored in the packet before border-casting it. In order to decrease overhead on intermediate nodes, the signing process is carried out by the source of the packet in the route request packet and by the destination for the route replay packet. This may lead to a problem in the verification of the route replay. The problem will appear if the RREP packet is generated by an intermediate node which has the link to the destination. To avoid this problem, we restrict the generation of RREP message to the destination only, while intermediate nodes behave as they didn't have the route and forward the RREQ message. Although this may lead to significantly increase in the response time, it will decrease the overhead of the verification process.

- **IERP Hashing**

SZRP uses hashing to attain the integrity of the packets since authentication of data in routing packets is not sufficient, as an attacker could remove a node from the node list. Hashing is performed on the mutable fields of IERP packets, the digest obtained is appended to the packet, and the packet is border-casted. The digest is used to allow every node that receives the message, either an intermediate node or the final destination node, to verify that these fields and especially the route to the destination haven't been altered by adversary nodes.

- **Secure IERP Scenario**

Every time a node requires a route to a destination but doesn't have the route stored in its route table, it initiates a RREQ packet with the format shown in figure 4.5, sets the Query ID to a new identifier that it hasn't recently used in initiating a route discovery. Query/Route source address and query/route destination address are set to the addresses of the source and destination, respectively. The source then computes the digital signature of the non-mutable fields and the hash value of its public key, appends them to the signature and digest fields, and border-casts the packet to its peripheral nodes. When any node receives the packet for which it is not the target node, it checks its local table from recent requests it has received to determine if it has already seen a request

from this same source. If it has, the node discards the packet; otherwise, the node checks the node list to be sure that the last node is already a node in its zone with a high trust level. Then the received node performs hashing on the packet and compares the result with the digest value to verify the integrity of the packet. Once the packet is accepted, the node modifies the request by appending its own address, A, to the node list and replacing the digest field with H[A,digest], then the node border-casts the packet. The scenario of securing route request packet is shown in figure 4.6.

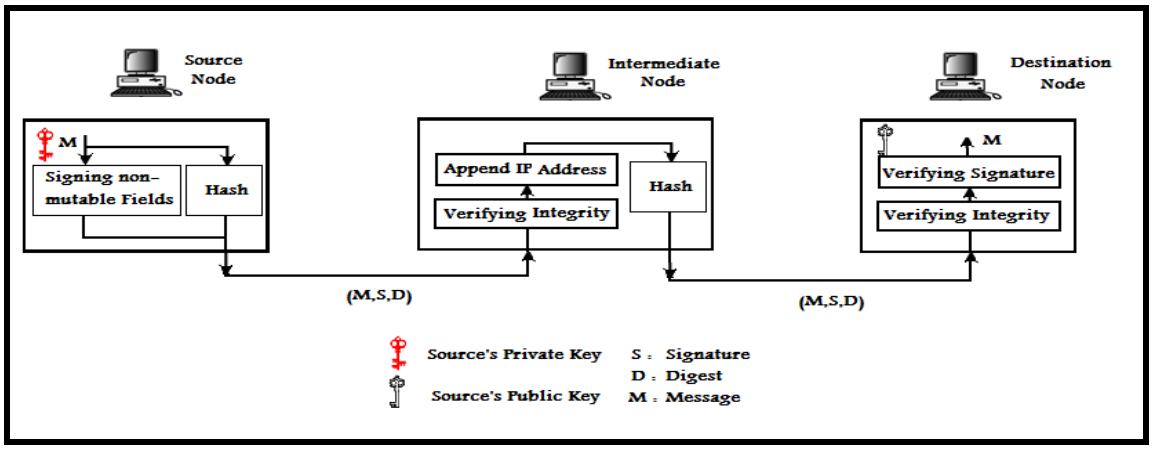


Figure 4.6: Secure IEPR scenario

When the destination node receives the route request, it checks the authenticity of the RREQ by verifying the signature using the private key of the source. The integrity of the packet is verified by determining that the digest is equal to:

$$H[n_n,H[n_{n-1},H[n_{n-2},....H[n_1, signature]]$$

Where n is the number of nodes in the node, n_i is the node address at position i in the list. If the destination verifies that the request is valid, it returns a route reply packet to the sender; this packet has the same format of route request packet except the packet type filed. All fields are set to the corresponding values in the same manner as described in the route request phase. This packet is then returned to the source along the source route obtained by reversing the sequence of node list stored in route request packet. Here, there is no need to perform hashing at intermediate node because it only unicasts the packet to the next hop as listed in the node list. When the source receives the route replay, it verifies the authenticity and integrity of the packet since no changes are added through transmission. If all the verifications are ok, it accepts the packets, otherwise it

rejects it. Figure 4.7 shows an example of message flow in the discovery of route {A,B,C} between source S and destination D.

S		:	$Signature=RSA_{K_S^-}(non\text{-}mutable(IERP\ RREQ))$
			$h_o=H[signature]$
S	→*	:	$< IERP\ RREQ,\ ho,\ signature,(\ )>$
A		:	$h_1=H[A,\ h_o]$
A	→*	:	$< IERP\ RREQ,\ h_1,\ signature,\ (A)>$
B		:	$h_2=H[A,\ h_1]$
B	→*	:	$< IERP\ RREQ,\ h_2,\ signature,\ (A,B)>$
C		:	$h_3=H[C,\ h_2]$
C	→*	:	$< IERP\ RREQ,\ h_2,\ signature,\ (A,B,C)>$
D		:	$Signature=RSA_{K_D^-}(IERP\ RREP))$
			$h_o=H[signature]$
D	→C	:	$< IERP\ RREP,\ h_o,\ signature,(A,B,C\ )>$
C	→B	:	$< IERP\ RREP,\ h_o,\ signature,(A,B,C\ )>$
B	→A	:	$< IERP\ RREP,\ h_o,\ signature,(A,B,C\ )>$
A	→S	:	$< IERP\ RREP,\ h_o,\ signature,(A,B,C\ )>$

Figure 4.7: Route discovery example

*** Incdicates bordercast address**

4.9 Detecting Malicious Nodes

Misbehaving nodes can affect network throughput adversely in worst-case scenarios. Most existing ad-hoc routing protocols do not include any mechanism to identify misbehaving nodes. It is necessary to clearly define misbehaving nodes in order to prevent false positives. It may be possible that a node appears to be misbehaving when it is actually encountering a temporary problem such as overload or low battery. Some work has been done to secure ad-hoc networks by using only misbehavior detection schemes. In this kind of approaches, it is too hard to guarantee the integrity and authentication of the routing messages. Therefore, secure routing protocols should provide the integrity and authenticity to the routing messages before being able to identify misbehaving nodes and isolate them during route discovery or updates operations.

In our design, we propose a new technique to deal with malicious nodes, and prevent them from further destroying the network. This technique is based on the available information produced by verification processes performed during transferring routing packets. It requires that each node maintains an additional field, trust level, to its neighbors table; this field is dynamically updated with the trust value of the corresponding node. The trust level is initialized with value 3 to indicate that a node is a trusted one. This level is decremented in three cases:

- The node initiates a HELLO message with wrong evidence or doesn't pass secure neighbor discovery protocol or,
- The packet sent by the corresponding node is dropped due to security verification failures, or
- The node provides a list with a non neighbor node.

In all, cases the value is decremented by one. The node is considered as a malicious node if the trust level value reaches zero. The malicious node is transferred to malicious table, and a new authenticated packet, "Alarm Packet", is generated that contains the packet type, the address of the malicious node, and the signature of both. The packet is transmitted in the same manner as IARP packet as described in algorithm 4.4. Each node receives the alarm packet reassigns the trust level of the malicious node stored in the packet to zero after verifying the authenticity. In future, each node doesn't perform any processing on the received packets until verifying the trust level of the sender.

Algorithm 4.4: Detecting Malicious Node

```
Input: node ID.
{
   Trust-level(ID)+=1
   If (Trust-level(ID)=3)
        Generate Alarm packet P
        Signature ←RSA_{K_S^+}(P).
        Append Signature to P.
        Broadcast P
        Add node ID to black-list
        Return 0
   End If
}
```

Chapter 5

VALIDATION OF SECURITY FUNCTIONALITIES OF SZRP

This chapter shows the validation of security functionalities of the proposed protocol by providing security analysis of RSA and SHA-1 systems in details and describes briefly how SZRP resists different attacks' types, according to the taxonomy we presented in section 3.3.

5.1 Security Analysis

In this section, we will present a formal security analysis of SZRP, evaluates its robustness in the presence of the attacks introduced previously, and verify that the stated goals are achieved.

5.1.1 Security Analysis of Digital Signature

Digital signature is based on asymmetric key cryptography (RSA), which involves more computation overhead in signing/verifying operations. Most researches claim that digital signature, in general, is less resilient against DoS attacks since an attacker may feed a victim node with a large number of bogus signatures to exhaust the victim’s computation resources for verifying them. However, we take this point into account when we design our protocol. Each node will not verify a message until it verifies the authentication of the transmitted node. Also a message from a malicious node will not be verified more than three times. After wrong verifications, malicious node will be stored in the black list, and won't be able to consume the resources of this node or other nodes.

Digital signature can be verified by any receiver having the public key of the sender. This makes this type applicable for broadcasting messages. Conversely, symmetric key systems and keyed hash functions can be verified only by the intended receiver, making it unappealing for broadcast message authentication, and only used in unicast authentication. Also, this makes digital signature scalable to large numbers of receivers. Only a total number of n public/private key pairs is required compared with symmetric-

key cryptography or keyed hash functions that require n (n-1)/2 keys to be maintained in a network with n nodes where establishing these secret keys between any two nodes is a nontrivial problem. Figure 5.1 shows the required number of keys for both symmetric cryptosystem and digital signature. One can easily note that secure protocols that are based on shared key aren't scalable to large number of nodes, keeping in mind that the processes of managing and distributing these keys will be more complex.

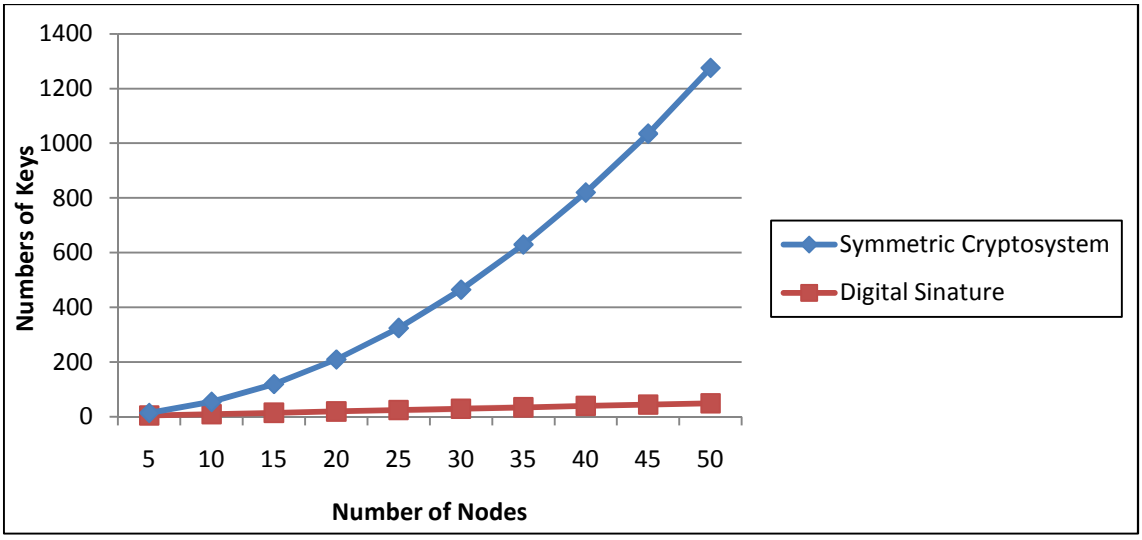


Figure 5.1: Number of required keys against the number of nodes

5.1.2 Security Analysis of RSA System

No devastating attacks on RSA have been discovered. Several attacks have been predicted based on week plaintext or weak parameter selections which are not present in our design; the plaintext is strong enough since it has a length of 512 bits.

- RSA is secure against factorization attacks since none of the available factorization algorithms has the ability to factor a large integer; it has a complexity of 2^{128} which means it needs 2^{98} seconds on a computer that can perform 1-billion bit operations per second.
- RSA is secure against attacks on the encryption exponent because we have used an encryption exponent e of 17 bits that is recommended by NIST Special Publication (SP 800-76-1), 2007 [65] to resist all types of this attack such as broadcast attacks, related message attacks, and short pad attacks [57].

- RSA is secure against attacks on the decryption exponent because we have d of 128 bits which is greater than $1/3n^{1/4}$ as recommended. However, if the value of d is leaked in any way, the node must immediately change n , e and d.

5.1.3 Security Analysis of Unique Identifier Addresses

- **Hash ID Size Consideration**

In unique identifier addresses, the lower 32 bits are reserved for the IP address, and 32 bits are usable as a hash value. However, the hash function produces 160-bits before performing XOR operations on it. So for the 160 bits, if an attacker tries to find the input that produces the same target output, he should try 2^{159} possible input values on average; each input with 512 bits long.

According to the size of the hash function, we shouldn't be worried about address duplications, this is because we need a population of $1.2*2^{160}$ nodes on average before any two nodes produce duplicate address (according to birthday paradox). Although this is very unlikely, duplicate address detection protocol will detect it, and the node will choose another IP address.

Impersonation attacks to UI are also very expensive operation. An attacker must attempt 2^{159} tries to find a public key that have the same hash value. If the attacker can perform one million hashes per second, it will need 2^{34} years. Additionally, an attacker must also generate a valid public and private key which is also very expensive as we will discuss shortly.

- **Key Size Consideration**

If an attacker finds a RSA public/private key pair that hashes to the same least 32-bits of UI, it can impersonate the mobile node. This can be achieved by a brute force attack. The attacker tries several public keys as input to the hash function used to generate the UI. The difficulty of this attack depends on the size of the modulus n used in generating this public/private key as discussed the previous section. This is a difficult task because the attacker must generate valid public/private key pairs before performing the hash function. If an attacker can find the public/private key pair that is used to generate the UI, an attacker can impersonate a mobile node and break the RSA system.

5.2 Thwarting the effect of Different Types of Attacks

After showing that breaking the security of the proposed mechanisms is not an easy task, we will analyze the reaction of our secure protocol in the presence of different kinds of attacks that threaten the routing protocols. We are listing a set of potential attacks where one or multiple nodes could perform in MANETs.

In all of the following schemes, {N1, N2, N3} represent cooperative nodes, and {A1, A2} represent attackers. We use four scenarios that present few examples of different types of attacks: modification, dropping, spoofing, and denial of service.

- **Modification Attacks**

Lengthen/shorten the route: An attacker, A1, between N1 and N2 as in figure 5.2 can receive the RREQ/IARP packets and add itself or a compromised node to the node list of the route in order to make the route going through longer and thus less attractive. Or an attacker can receive RREQ/IARP packets and remove a node from the node list to make the route going through shorter and thus diverts all traffics through it.

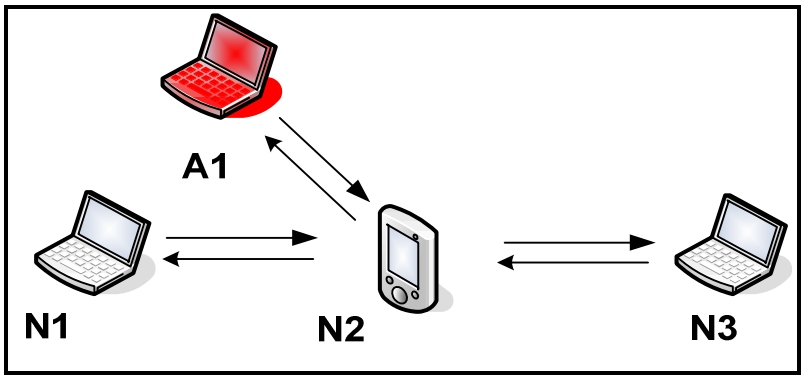


Figure 5.2: Modification attack – type 1

In SZRP, an attacker can't add a node to the node list without being an authenticated neighbor to the receiver node. N3 will detect that A1 is not a neighbor, and hence drops the packet before performing any processing on this packet. In case that the attacker is already a neighbor to N3 and can pass neighbor verification mechanism, which rarely happens, verification of the integrity/authenticity of RREQ/IARP will detect that the compromised node or the attacker have been illegally added to the route, and hence the packet will be dropped. Once the packet is dropped, an alarm packet will be sent to all nodes indicates that A1 is an attacker to prevent it from further injecting false packets.

This scenario of alarm packets will be repeated whenever a packet is dropped due to verification failure.

Deviating the route by modifying DSN: An attacker can receive RREQ sent by the source N1 in figure 5.3, replay with a greater destination sequence number to N2 which will discard all subsequent traffic destined for the destination N3.

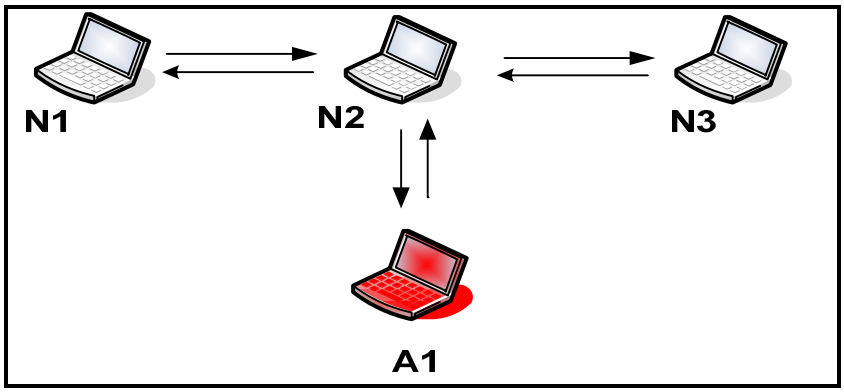


Figure 5.3: Modification attack –type 2

Our proposed protocol prevents this type of attacks by restricting the initiating of the RREP packet to the destination who will sign it using its private key. Once the attacker tries to receive the RREP, modify the DSN, it will be detected through verification process of N2, and thus the packet will be dropped.

- **Dropping Attacks**

A malicious node can decide to drop some or all the packets it has to forward from N1 to N3 as in figure 5.4.

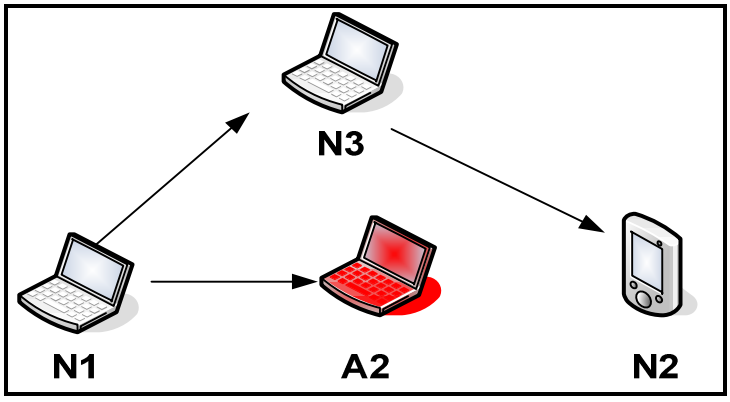


Figure 5.4: Drooping attack

This type of attacks can't be countered in SZRP. However, it doesn't have a significant impact in dense networks because the control of packet flooding provides the required robustness, e.g. N2 can receive the same packets from N3, or other surrounding nodes.

- **Spoofing Attacks**

An attacker receiving a RREQ can mislead N2 in figure 5.5 by generating RREP with less number of nodes in the list other than any legitimate reply. It also will be received with the least delay because of the close distance between the attacker and N2.

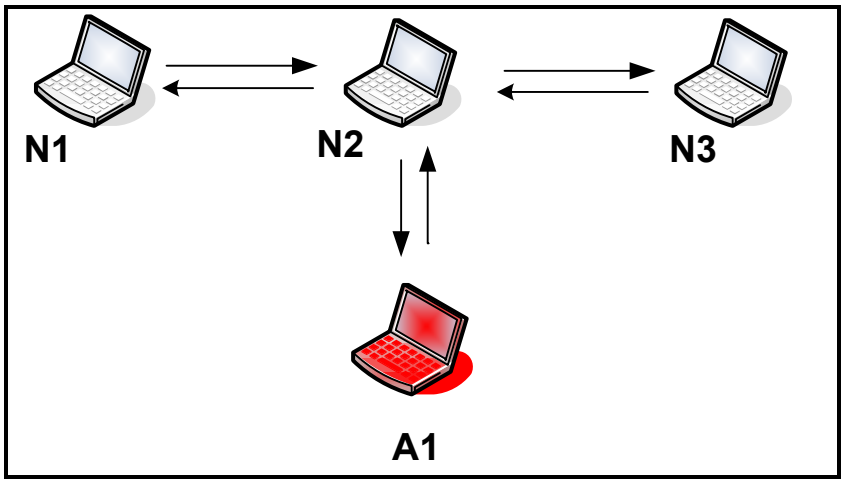


Figure 5.5: Spoofing attack

This type of attacking is thwarted by the disallowance mechanism that prevents any intermediate node from generating RREP because the sender will discard replies except from the destination. If the attacker tries to generate the reply claiming that he is the destination, the generated packet will be discarded because the attacker doesn't have the private key of the destination and thus can't generate a valid signature.

- **Replay Attack**

An attacker might want to mount a replay attack for packets. Replayed requests will be detected at the destination and replayed replies will be detected at source by using standard mechanisms of the conventional ZRP based on destination sequence numbers and query ID.

- **Impersonating Attacks**

Impersonating attacks can't be launched in our SZRP. An attacker that has not compromised any node (and hence does not possess any cryptographic keys from a node) cannot successfully send any routing messages impersonating any other node, since an uncompromised neighbor node will reject the messages due to the failed neighbor authentication.

- **Denial of Service Attacks**

Denial of Service (DoS) is a very common attack; it may slow down or totally interrupt the overall network. The attacker can use several strategies to achieve this goal and exhaust node resources such as memory and computation resources as the node has to authenticate packet signatures and the digest, while these mechanisms are computationally intensive operations.

Beacon Acknowledge Storm: one of DoS attacks is to send a storm of beacon acknowledge messages to a victim node, allowing the node to perform numbers of operations. We prevent this type of attacks by inserting evidence to the beacon message. If the node receives a beacon acknowledge with an evidence that isn't equal to what has been sent in the beacon message the beacon acknowledge will be rejected before performing verification process.

IAPR storm: Malicious node could try to attack its neighbors by sending a storm of IARP update packets with false data to consume the node's resources in computing the new routes, and updating its neighbor table. This type of DoS attack is prevented by using digital signature and detection of malicious node mechanisms. Digital signature will check the authenticity of the node and the integrity of the received packets by comparing the node ID with those nodes stored in its neighbor table and performing digital verification using the stored public key of the sender.

If three packets are rejected from any cooperative node, an alarm packet will be broadcasted to add this malicious node to the black list. Any received packet from malicious nodes will be dropped without performing any processing on it. This

mechanism prevents malicious nodes from further degrading the performance of the network.

RREQ Storm: Malicious node could try to attack a node by sending a storm of RREQ packets to a victim node to consume their resources. This type of DoS attacks can be easily prevented by using the trust level value of the malicious node as discussed above in IARP storm, or checking the authenticity of the malicious node by the destination node. In both cases, the packet will be rejected if it is proved that the node is not a legitimate one.

In general, malicious node detection mechanism protects the network against all kinds of denial of service attacks. This mechanism is always performed as a first check in order to decrease the overhead produced by signature verification. Once malicious node is detected, the verifier will drop the packet before performing any farther processing.

5.3 Thwarting the Effects of Well-Known Attacks

***Rushing Attack*:** attacker forwards packets beyond the normal radio transmission range using its higher gain antenna, or a higher power level in order to suppress any subsequent packet. The proposed protocol defends against rushing attack by using secure neighbor detection that allows both the sender and the receiver to verify that the other party is within the normal direct wireless communication range.

Wormhole Attack: One of the most severe attacks on MANETs is wormhole attack. The major cause of this attack is the absence of any neighbor detection mechanism. In the wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. The wormhole attack can be detected by an unalterable and independent physical metric, such as time delay or geographical location where both are provided through secure neighbor discovery mechanism. We detect the wormhole attacks through this phase to reduce the overhead and delay produced if the detecting of the wormhole attacks is performed during packet transmission.

Chapter 6

PERFORMANCE EVALUATION

This chapter presents an evaluation of the proposed protocol. To evaluate our protocol, we analyze the cost and effectiveness through simulation by presenting the cost of applying our proposed mechanisms to a non-adversarial environment as proposed in most secure routing protocols [8-11], and provide a full analysis of the simulation results obtained.

6.1 Simulation Environment

To evaluate our SZRP in a non-adversarial environment, we have used the Network Simulator 2 (NS-2) [37]. NS-2 is a discrete event simulator written in C++ and OTcl. It was developed by the University of California at Berkeley for simulating the behavior of network and transport layer protocols in a complex network topology. It has been used extensively in evaluating the performance of ad-hoc routing protocols. It realistically model arbitrary node mobility as well as physical radio propagation effects such as signal strength, interference, capture effect, and wireless propagation delay. At the link layer, the simulator implements the complete IEEE 802.11 standard Medium Access Control (MAC) protocol.

We modeled our SZRP by modifying the existing ZRP in several ways:

- We increased the packet size to reflect the additional fields necessary to perform security mechanisms. The extended fields hold the public key, the digest, the unique identifier, and the signature. One should note that not all packets hold these fields.
- We increased the size of the neighbor table of each node by two fields; the first filed is used to store the public key of its neighbors in each entry, while the other is used to indicate the trust level factor of that neighbor.
- We created new packet called "Alarm Packet" that is generated and broadcasted to declare malicious nodes when the trusted level value reaches zero as discussed in section 4.8.

6.2 Mobility Model

Each node in our experiments moves according to the random waypoint model [3], in which each node begins at a random location and moves independently during the simulation. Each node remains stationary for a specified period that we call the pause time and then moves in a straight line to some new randomly chosen location with a velocity uniformly chosen between 0 and v_{max}. Once reaching that new location, the node again remains stationary for the pause time, and then chooses a new random location to proceed to at some new randomly chosen velocity, the node continues to repeat this behavior throughout the simulation run. This model can produce large amounts of relative node movements and network topology change, and thus provides a good movement model with which to stress any MANETs routing protocols. This mobility scenario was generated using CMU's TCP/CBR traffic scenario generator.

6.3 Communication Patterns

The data communication pattern in our experiments uses four source-destination pairs, each sending a Constant Bit Rate (CBR) flow of four data packets per second. A rectangular space of size 1500×500 m^2 is used to increase the average number of hops in route used. A rectangular space is recommended in most proposed work to evaluate MANETs routing protocols as in [8, 9] relative to square space of equal area. It creates a more challenging environment for the routing protocol. Other simulation parameters used are presented in table 6.1 below, where we tried to select them similar to other simulations related to secure MANETs protocols [8-14, 46].

Number of nodes	25
Maximum velocity	20 m/s
Dimension of space	1500×500 m^2
Nominal radio range	250 m
Source- Destination pairs	4
Source data rate	5 packets /s
Simulation time	500 s
Zone radius	3 hops
Hash length	160 bits
Signature length	160 bits
Public key length	160 bits

Table 6.1: Parameters for studying the performance of SZRP

6.4 Performance Metrics

We evaluate our proposed protocol by comparing it with the current version of ZRP [6]. Both protocols are run on identical movements and communication scenarios; the primary metrics used for evaluating the performance of SZRP are packet delivery ratio, routing overhead in bytes, routing overhead in packets, and end-to-end latency. These metrics are obtained from enhancing the trace files.

- ***Packet delivery Ratio:*** This is the fraction of the data packets generated by the CBR sources to those delivered to the destination. This evaluates the ability of the protocol to discover routes.
- ***Routing overhead (bytes):*** This is the ratio of overhead bytes to the delivered data bytes. The transmission at each hop along the route is counted as one transmission in the calculation of this metric. The routing overhead of a simulation run is calculated as the number of routing bytes generated by the routing agent of all the nodes in the simulation run. This metric has a high value in secure protocols due to the hash value or signature stored in the packet.
- ***Routing overhead (packets):*** this is the ratio of control packet overhead to data packet overhead over all hops. It differs from the routing overhead in bytes since in MANETs if the messages are too large, they will be split into several packets. This metric is always high even in unsecure routing protocols due to control packets used to discover or maintain routes such as IARP and IERP packets.
- ***Average End-to-End latency:*** This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes.

6.5 Simulation Results

We simulated our SZRP over four scenarios to evaluate it through different movement patterns, network size, transmission rate, and the radius of the zone.

6.5.1 Performance against Different Mobility Networks

In this scenario, we compare the SZRP and ZRP over different values of the pause time. The pause time was changed from 100 s to 500 s to simulate high and low mobility networks. Figures 6.1 to 6.4 show the observed results.

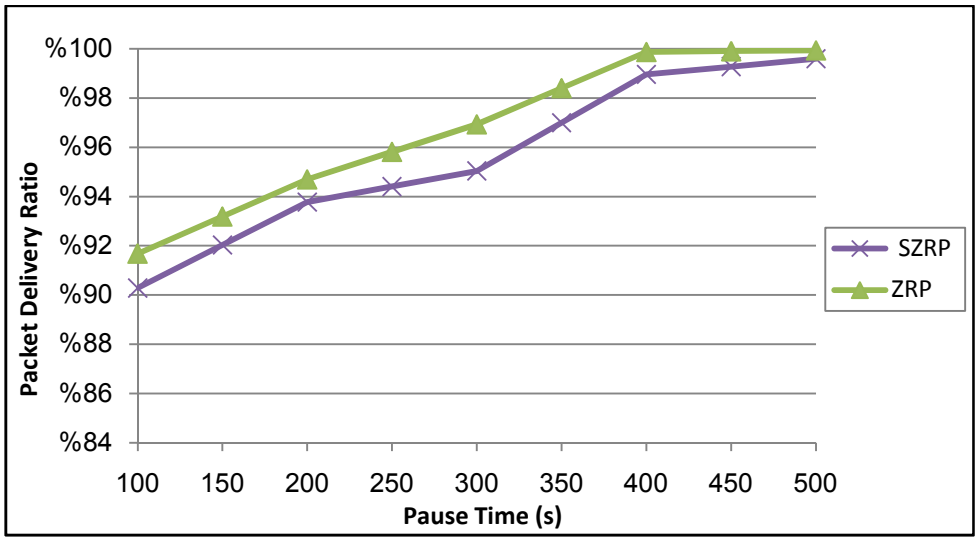


Figure 6.1: Performance of packet delivery ratio against pause time

Figure 6.1 illustrates the results of the packet delivery ratio as a function of pause time. The result shows that the packet delivery ratio obtained using SZRP is above 90% in all scenarios and almost similar to the performance of ZRP. This indicates that the SZRP is highly effective in discovering and maintaining routes for the delivery of data packets, even with relatively high mobility network (low pause time). A network with high mobility nodes has a lower packet delivery ratio because nodes change their location through transmitting data packets that have the predetermined path. For this reason, a high mobility network has a high number of dropped packets due to TTL expiration or link break.

Figure 6.2 explores the extra routing overhead introduced by both SZRP and ZRP. The routing overhead is measured in bytes for both protocols. The result shows that the routing overhead of SZRP is significantly higher and increased to nearly 42% for a high mobility network and 27% for a low mobility network. This is due to the increase in size of each packet from the addition of the digest and the signature stored in the packets to verify the integrity and authentication. This routing overhead decreases as the

mobility decreases duo to increase of the number of updating packets required to keep track of the changes in the topology in order to maintain routing table up-to-date. These packets include both IARP and IERP packets as well as the error messages.

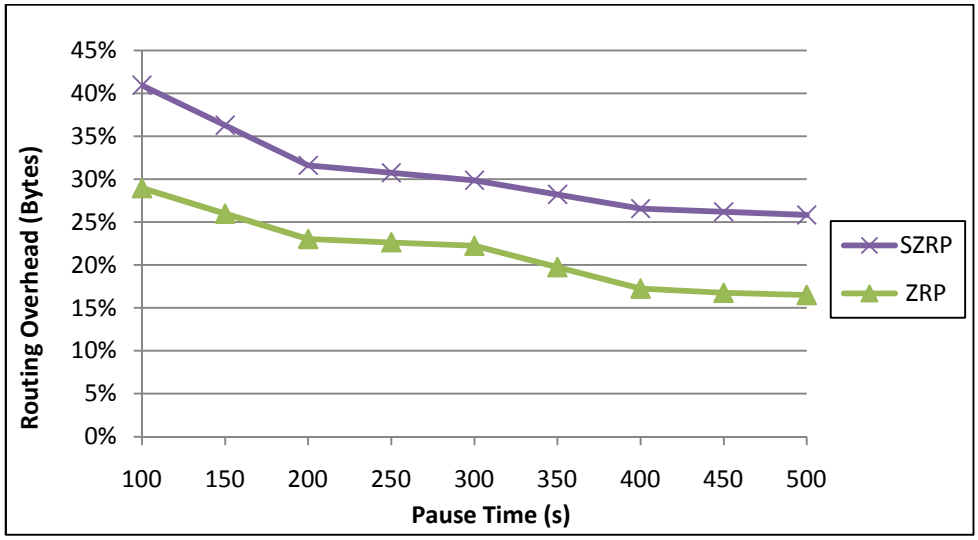


Figure 6.2: Performance of routing overhead in bytes against pause time

The ratio of routing overhead due to control packets transmitted by both protocols in the same simulation environment is shown in figure 6.3. The result obtained confirms the previous result of byte overhead. The routing packet decreases for both protocols in the same manner. The ratio of SZRP is higher because of the new messages used in secure neighbor detection schemes as well as the packets produced by splitting the control packets whenever the number of bytes in a packet exceeds a threshold value.

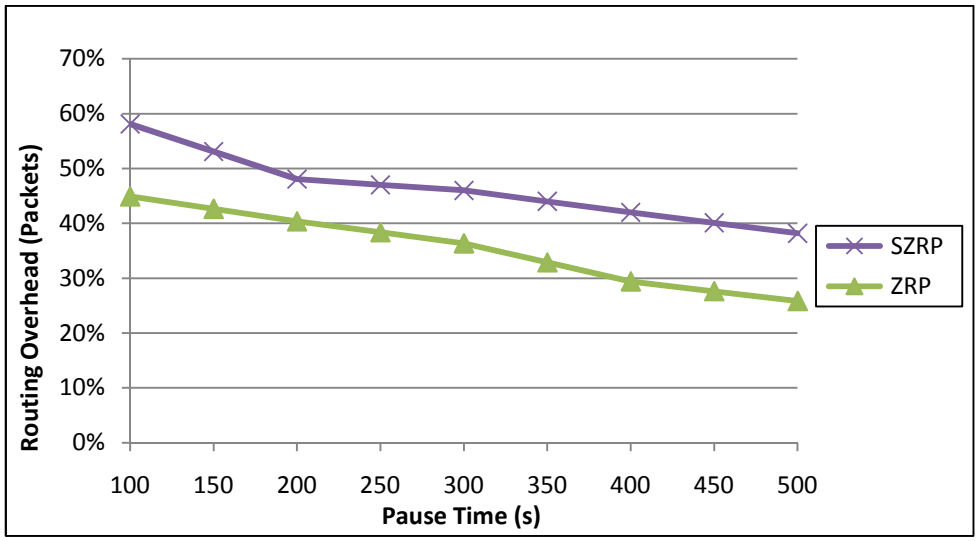


Figure 6.3: Performance ofrouting overhead in packets against pause time

The end-to-end latency for both protocols is shown in figure 6.4. The average latency of SZRP is approximately double that of ZRP due to the decreased of the available network capacity that is caused by the extra packets and bytes generated for security issues in SZRP. Furthermore, each node has to verify the digital signature and the digest produced by its previous node, compute the newest ones, and insert those values in the packet before retransmission. These signature and hashing processes cause an additional delay in processing the received data packets. The rise in latency at low pause times is due to the non-uniform distribution of nodes in space caused by node motion in the random waypoint.

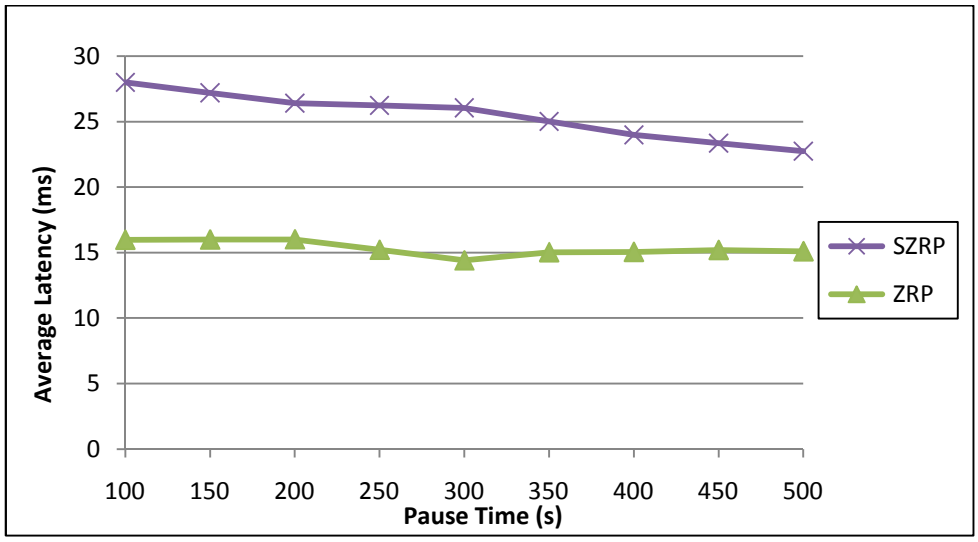


Figure 6.4: Performance of average latency against pause time

6.5.2 Performance against Different Data Rates and Mobility Patterns

In this scenario, we compare the SZRP and ZRP over different values of data rate. We considered these values since high data rate is always an imperative need in any network although it has an extreme effect in increasing the congestion in MANETs. The data rate was changed from one to nine packets per second. These scenarios are performed under high and low mobility networks, 100 s and 500 s, respectively. Figures 6.5 to 6.8 show the collected results.

Figure 6.5 shows the packet delivery ratio of SZRP and ZRP for both low and high mobility networks. We note that the packet delivery ratio exceeds 89% in all cases

which can be considered as a good indicator that SZRP goes in the same manner as the conventional ZRP. The delivery packet ratio of low mobility networks increases as the data rate increases as expected since the discovered route to the destination will not change during transmitting the packets, and thus the success of delivering the packet to the same destination will increase. On the other hand, the packet delivery ratio decreases in high mobility networks as the data rate increases because of the high probability of congestion by both the increased data packets and the increased control messages needed to maintain the network nodes up-to-date with the changeable topology.

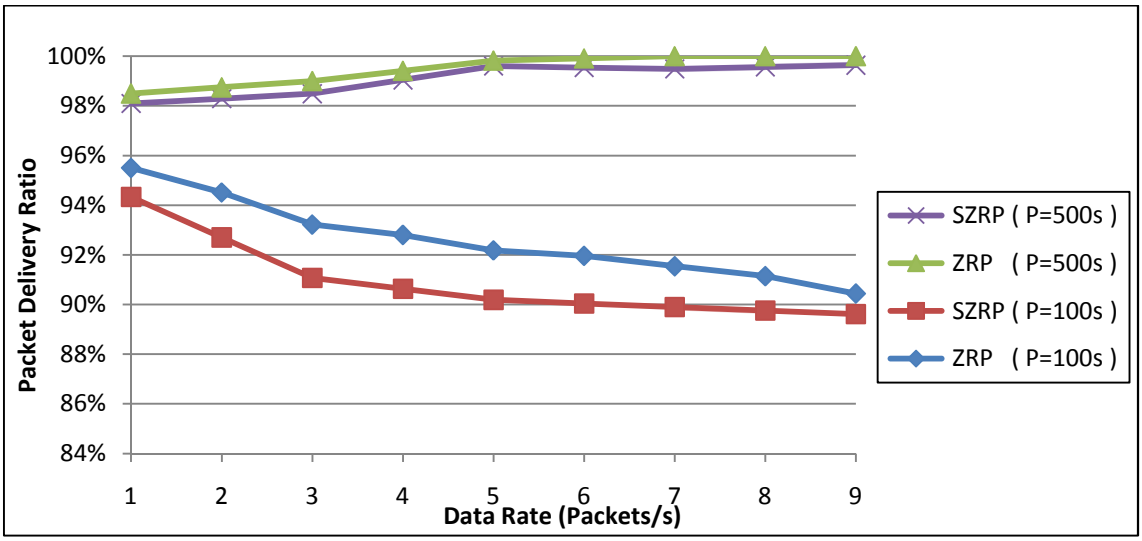


Figure 6.5: Performance of packet delivery ratio against data rate

In figure 6.6, the results show that the routing overhead in bytes decreases as the data rate increases. This decrease is related to the increase of data rate all over the time and isn't significantly affected by the number of bytes used in securing the control messages. An interesting point that appears in these results is that the number of overhead bytes produced by SZRP is not affected by increasing the data rate which means that the proposed protocol can be applied to network with high and low data rate.

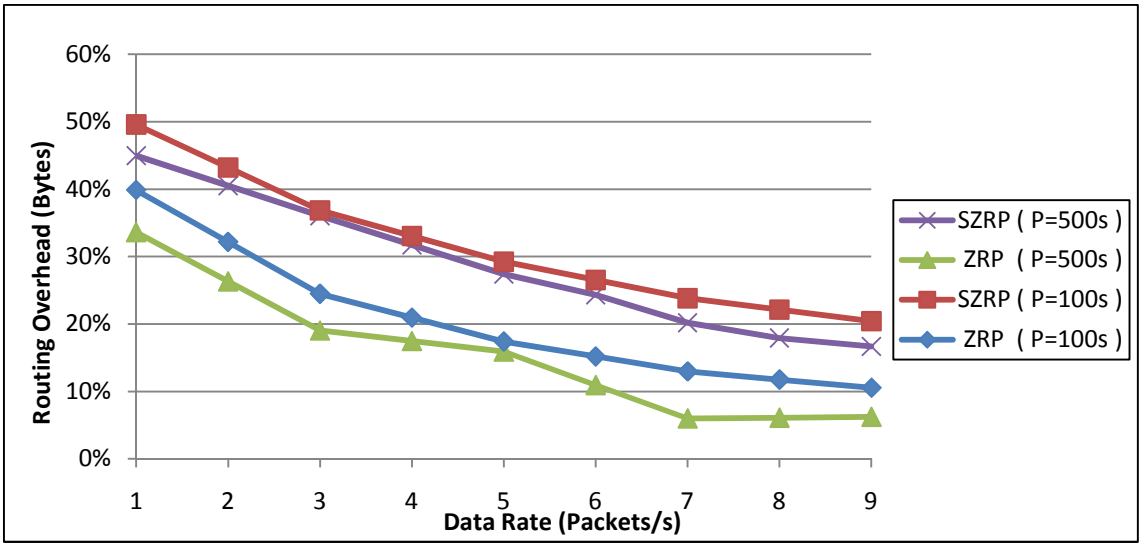


Figure 6.6: Performance of routing overhead in bytes against data rate

Figure 6.7 confirms the result obtained in the previous figure; no significant changes are observed since the topology of the network is not changing along different data rates. The routing overhead decreases in both protocols where SZRP in high and low mobility networks still has a higher routing overhead in packets than the conventional ZRP because of the additional packets and bytes used for security purpose.

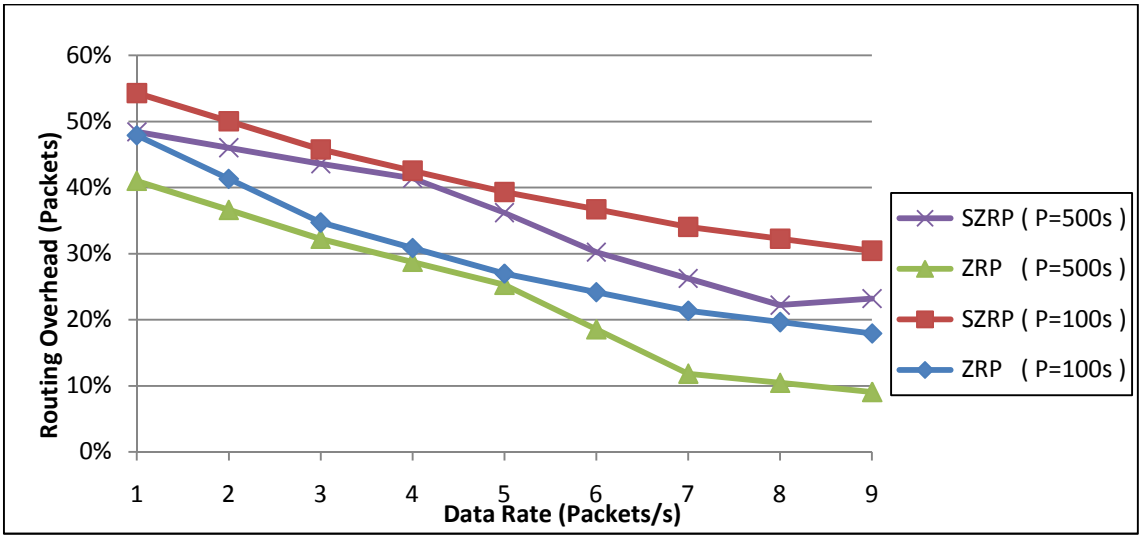


Figure 6.7: Performance of routing overhead in packets against data rate

The average end-to-end latency is illustrated in figure 6.8. Both protocols have a lower end-to-end latency in low mobility network. In general, the average latency is constant over the same scenario for low data rate, but it decreases in the high data rate according to the congestion occurred in the network because of the extra data packets sent every

second. SZRP with high mobility is worse since it has a higher overhead in routing packets which will cause an earlier congestion. This means that one should be aware when using SZRP in both high mobility and high data rate networks.

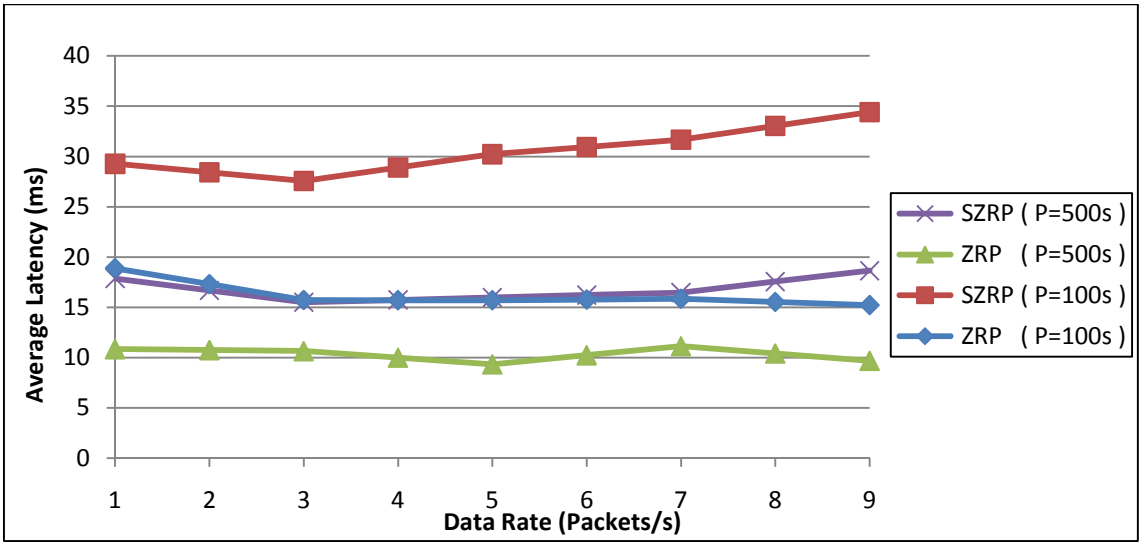


Figure 6.8: Performance of average latency against data rate

6.5.3 Performance against Different Network Sizes and Mobility Patterns

The third scenario studies the performance of SZRP and ZRP over different network sizes. The number of nodes changes from ten to forty in order to validate our secure routing protocol in different networks. The experiments are performed under high and low mobility rate with data rate of five packets per second. To be consistent, the dimension of the topology used is changed with the same ratio as the number of mobile nodes.

Figure 6.9 shows the performance of SZRP and ZRP in terms of packet delivery ratio. The SZRP still performs well in low mobility network where it exceeds 99%. However, its performance degrades in a high mobility network. In both cases, the result obtained is accepted because it degrades in the same manner as the conventional ZRP. A final point observed from this figure is that the packet delivery ratio decreases in a large network which is an expected result due to the increase of the traveling time that may lead to TTL expiration.

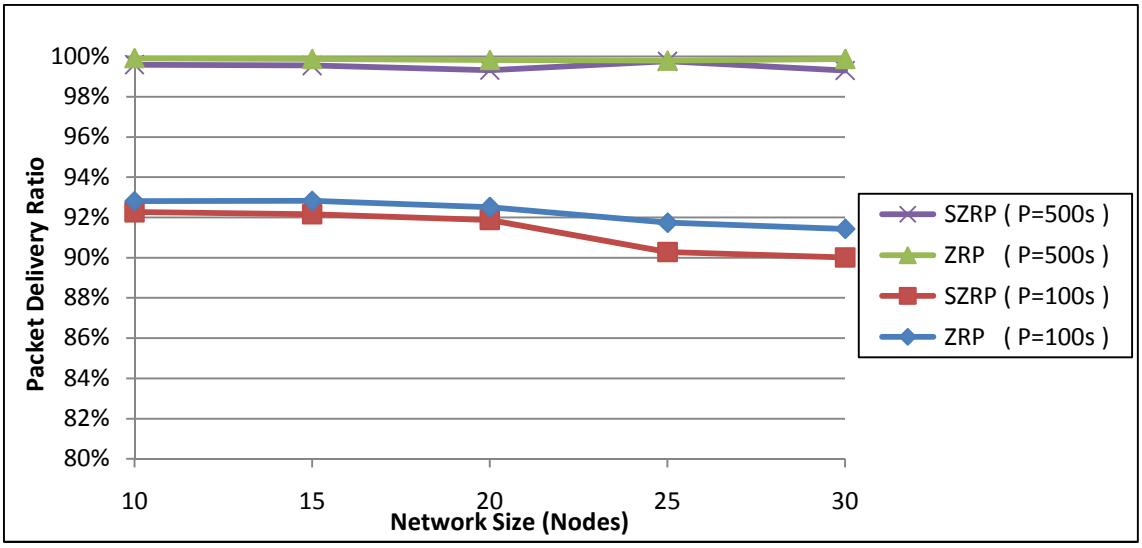


Figure 6.9: Performance of packet delivery ratio against network size

The routing overhead in bytes is shown in figure 6.10 for a changeable network size. The results show an increase in total bytes as the network size increases because of the increasing in the number of nodes that leads to escalate the degree of the routing activities in the network; more routing information is shared among the nodes as a result. SZRP has a higher overhead due to the increase of routing packets used to discover or maintain the routes, and the increase of the data needed to perform neighbor discovery mechanisms.

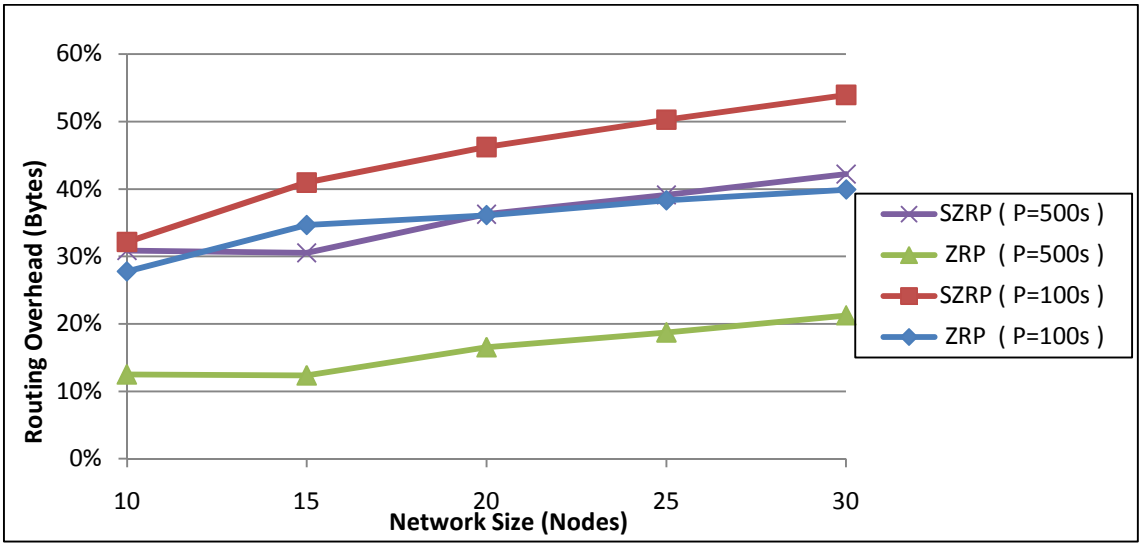


Figure 6.10: Performance of routing overhead in bytesagainst network size

The overall routing overhead in packets is shown in figure 6.11. The measurements show that both protocols have an increase in the packets overhead. This is because more

nodes are in a position to generate IARP updating messages and respond to the RREQ messages. However, the increase of SZRP over ZRP in the packets isn't too large as in bytes because the extra bytes generated are covered in the existing packets and no extra packets are needed to be generated.

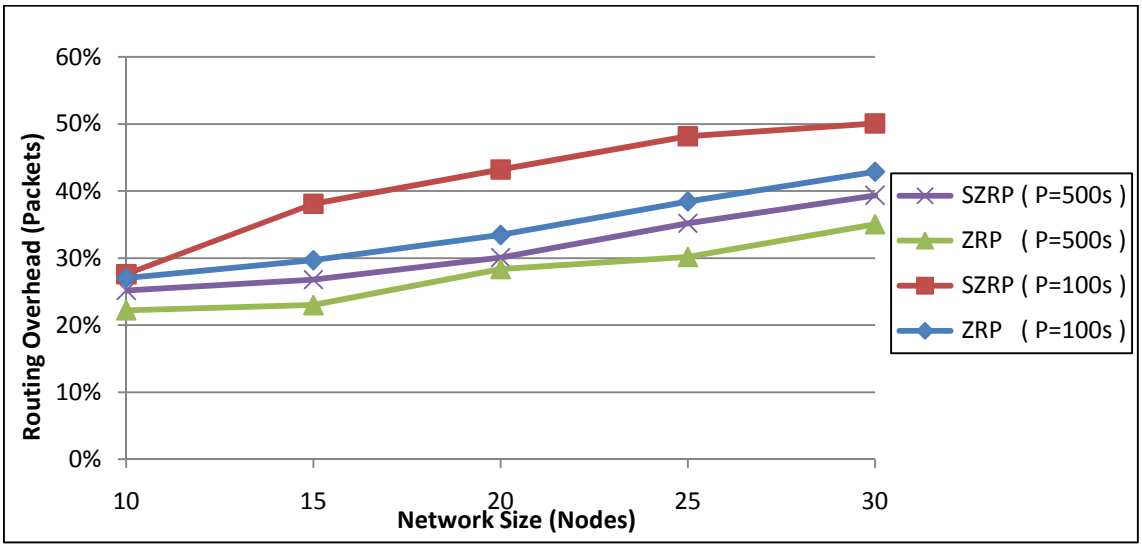


Figure 6.11: Performance of routing overhead in packetsagainst network size

The average end-to-end latency is shown in figure 6.12. The average latency increases with the increase of network size as well as the dimensions of the topology. SZRP has a higher latency due to the processing delay used to provide security requirements.

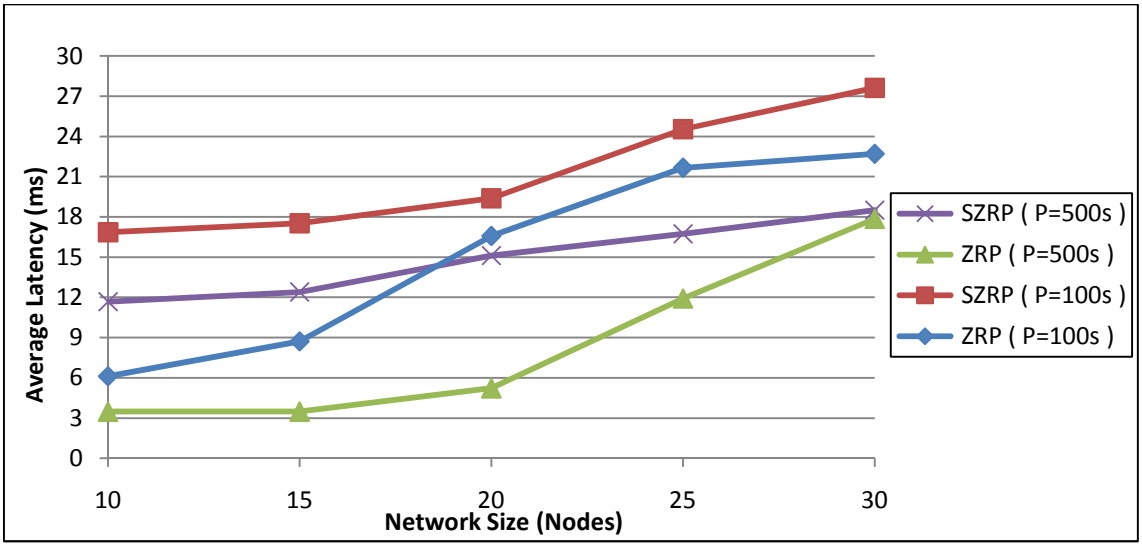


Figure 6.12: Performance of average latency against network size

The results obtained in preceding figure provide a clear indication that SZRP will match the performance of ZRP in large networks, because the difference of latency between them decreases as the network size increases in both high and low mobility networks. Although this may be at the expense of bytes and packets overhead, it will be acceptable in high bandwidth networks where the high transmission is an essential requirement.

6.5.4 Performance against Different Routing Zones and Mobility Patterns

The last scenario studies the performance of both protocols under different routing zones. The number of routing zone nodes can be regulated through adjustments in each node's transmitter power. To provide adequate network reachability, it is important that a node is connected to a sufficient number of neighbors. However, more is not necessarily better. As the transmitters' coverage areas grow larger, so do the membership of the routing zones, an excessive amount of update traffic may result.

Figure 6.13 shows that SZRP performs well in a different zone radius. It is obvious that both protocols aren't affected by the zone radius and still have the ability to discover the route to destination. In low zone radius, the two protocols behave like purely reactive protocol. They depend on route discovery mechanism to find the optimum route to the destination.

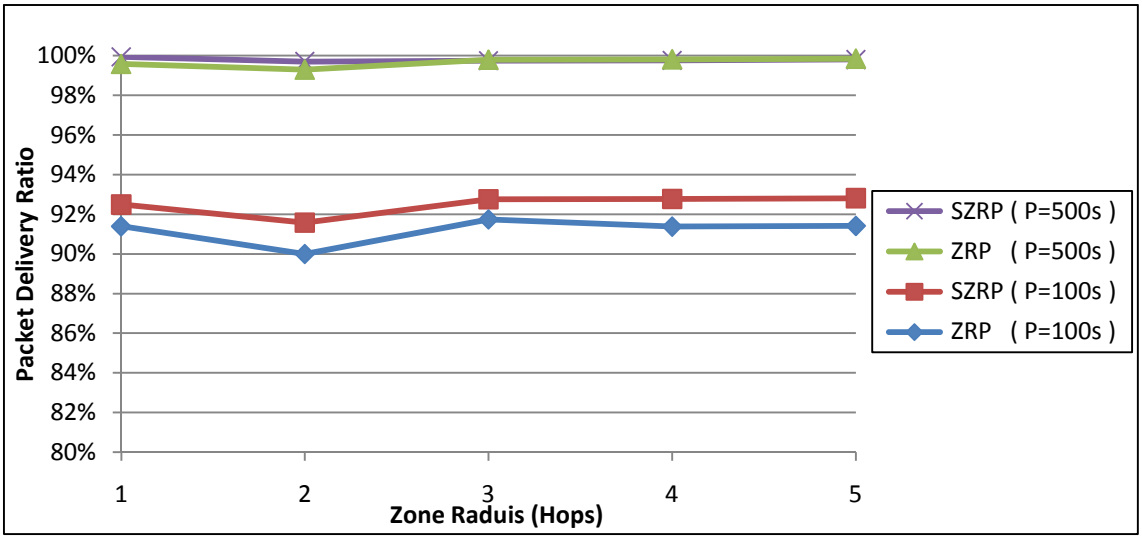


Figure 6.13: Performance of packet delivery ratio against zone raduis

The overhead produced by SZRP is illustrated in figure 6.14 as for ZRP. It is obvious that the overhead of packets decrease as the zone radius increases until reaching $\rho = 3$ which we can consider here as the optimal radius. Before reaching this value, the protocol behaves around purely reactive protocols where the IERP packets have the majority over all packets. We note that the packets overhead decreases with the increase of zone radius because of border-casting and query control mechanisms that allow queries to be directed to the edge of a routing zone, and thus reducing unnecessary queries within a routing zone. In addition, the packet overhead begins increasing when the zone radius exceeds the optimal because of the route update processes needed to notify neighbors about network topology. In all cases, the routing overhead is increased for high mobility networks because of the extra control packets needed to maintain the changeable locations of nodes.

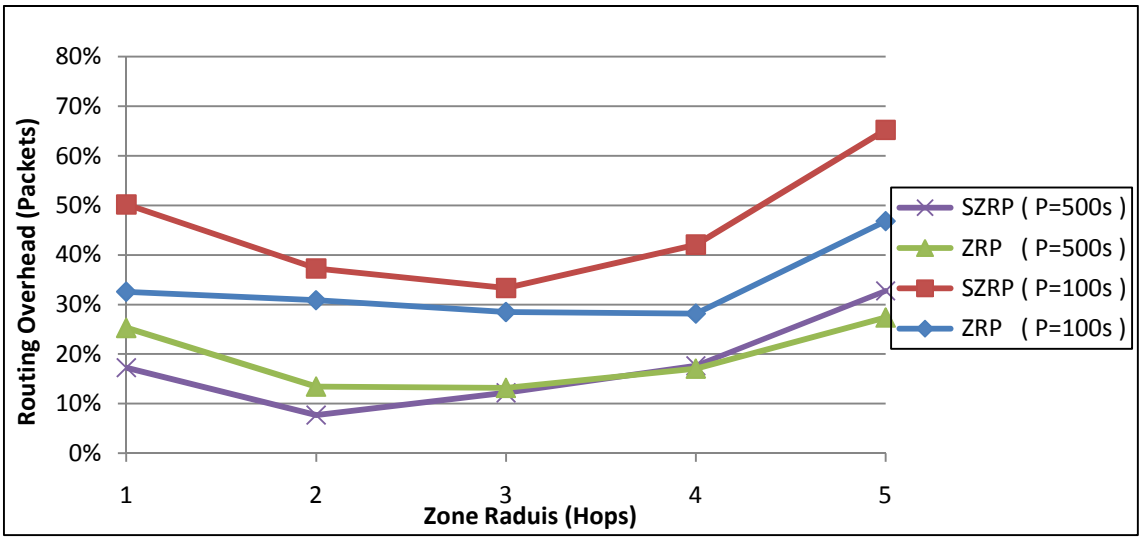


Figure 6.14: Performance of routing overhead in packets against zone radius

The results obtained in figure 6.15 confirm the previous discussion, the total overhead in bytes decreases until reaching the optimal zone radius, then it increases again. Both protocols have a higher overhead in a high mobility network because of the extra messages needed to maintain the changes of the topology. The SZRP provides extra overhead in bytes due to extra bytes used in both IARP and IERP packets for security. The difference between the two protocols is smaller in low zone radius. This is because both protocols behave like reactive protocol and the majority of overhead is related to the number of IERP packets which is relatively small since it is generated upon request.

So, the extra bytes needed aren't too large. Furthermore, the protocols depend on IARP packets in high zone radius which are generated periodically, and need a high number of bytes to provide the security requirements.

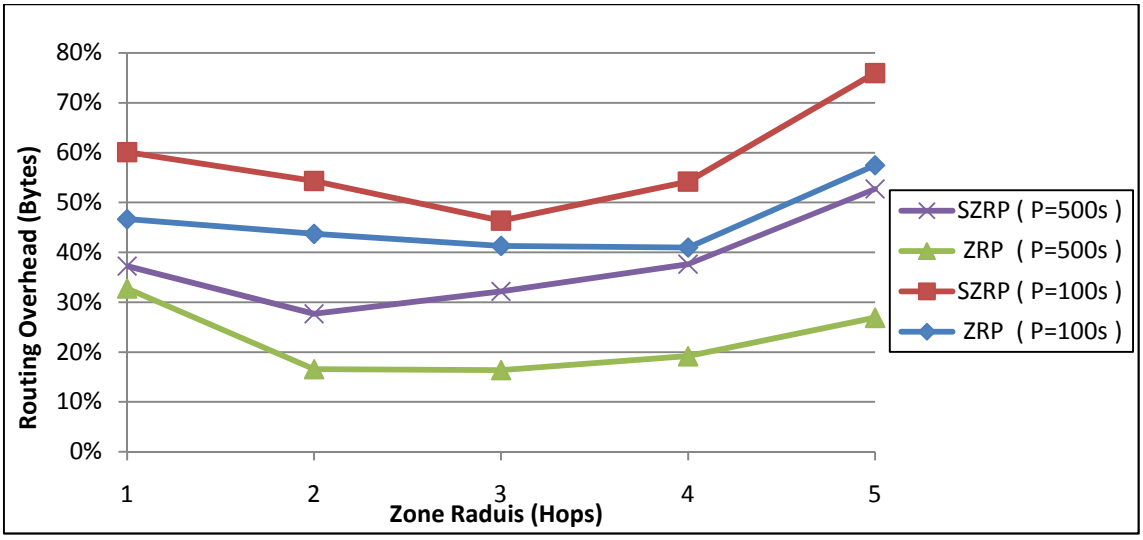


Figure 6.15: Performance of routing overhead in bytes against zone radius

The average end-to-end latency measured is illustrated in figure 6.16. The purely proactive protocols have the lowest latency because they keep the routing information up-to-date at the expense of large portion of the bandwidth. However, low zone radius networks have a higher delay because the nodes need more setup delay to discover the route, SZRP needs more time for extra processing needed to signing/verifying packets.

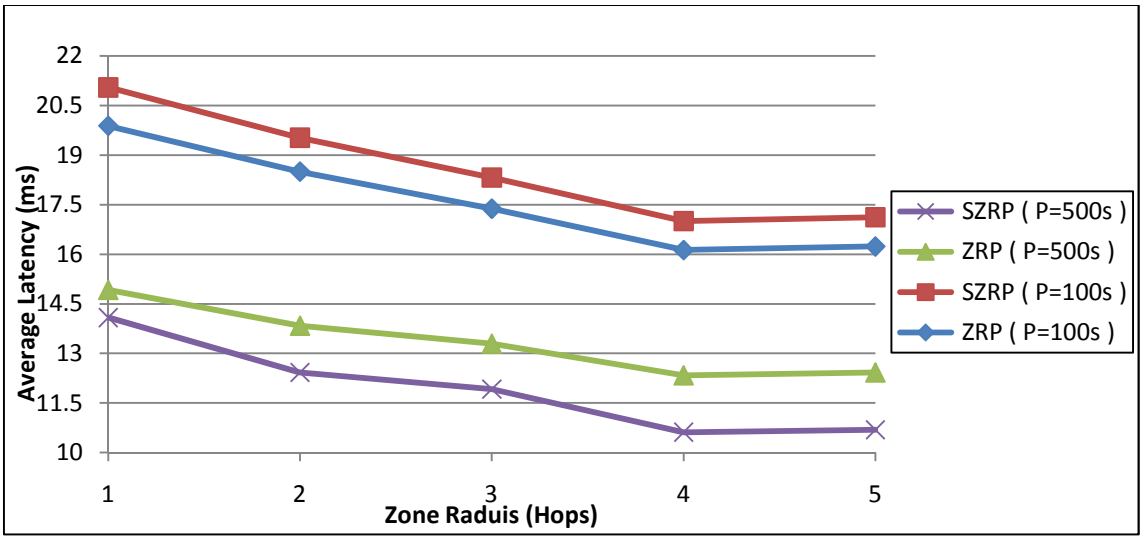


Figure 6.16: Performance of average latency against zone radius

6.6 Effect of Malicious Nodes Behavior

The experiments described in the previous sections compare the performance of SZRP and ZRP when all the nodes in the network are well-behaved. In order to validate our protocol against malicious nodes, we conducted additional experiments to determine the effect of malicious nodes behavior that generate invalid signature caused by any type of attacks discussed in chapter 3. We varied the number of malicious node from 0 to 5 nodes.

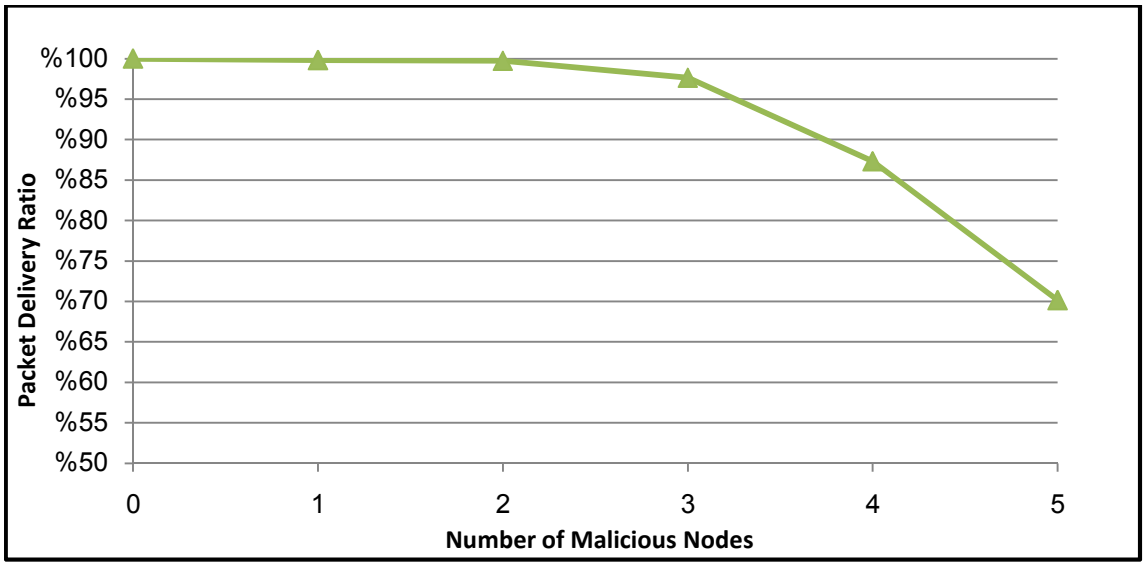


Figure 6.17: Effect of malicious modes behavior

Figure 6.17 shows the packet delivery ratio in the presence of malicious nodes. It is obvious that the number of malicious nodes has a significant effect on the packets that are successfully delivered to the destination. The packet delivery ratio is decreased as the number of malicious nodes increases. This is duo to the decrease in the available number of nodes that have the ability to provide the route to the destination or establish an alternative one. In general, SZRP still have the ability to deliver packets although the ratio of the malicious nodes reaches 20% of the network size

6.7 Summary of Our Results

Based on our performance evaluation, one can conclude that in non-adversarial environments, SZRP adds acceptable costs relative to ZRP, many of these cost are due to the congestion created and extra bytes/packets used for security requirements. This

cost is applicable as most proposed secure routing protocol [8-10]. Furthermore, our proposed protocol is highly effective in discovering and maintaining routes for the delivery of data packets where it has a high packet delivery ratio under all circumstances. Security analysis shows minutely that breaking the security of the system and launching the keys used is out of reach. It also emphasizes the ability of the protocol to resist known vulnerabilities of existing routing protocols and has the following advantages:

- It prevents most of the denial-of-service attacks by using a new mechanism of detecting malicious nodes.
- It prevents one of the most severe attacks on MANETs; wormhole and rushing attack, by using an efficient secure neighbor detection mechanism.
- It uses efficient hash function in hop-to-hop transmission in order to reduce overhead.

Chapter 7

CONCLUSION

This thesis was dedicated to demonstrate the security of zone routing protocol; a hybrid protocol that aims to address the problems of excess bandwidth and long route request delay of proactive and reactive routing protocols, respectively, although it is well suited for any hybrid routing protocol in MANETs. For this purpose, we surveyed several mobile ad-hoc routing protocols that assume trusted environment, and discussed various attacks against some of them. Also, we carefully analyzed the secured protocols proposed with respect to reactive and proactive routing protocols.

Four mechanisms are proposed in order to provide a comprehensive secure routing that can defend against all vulnerabilities in ad-hoc networks. The first mechanism is the identity-based key management that doesn't depend on any trusted key distribution center or certification authority that is rarely found in MANETs. This mechanism provides an identifier that has a strong cryptography binding with the public key of the node. The second mechanism provides a secure neighbor discovery to assure the correct view of neighbor information. It uses a combination of time and location to verify the discovery of legal nodes and prevent a malicious node from deluding other nodes that are within its radio transmission range, and thus preventing most famous attacks such as wormhole, rushing, and replays attacks. The core of the proposed protocol is relying on securing the control packets generated to performs route discover, route maintenance, and routing tables updates that provide through the third mechanism secure routing packets. Both digital signature and one-way hash function are used to achieve our goals. The final mechanism is based on detecting a malicious node using trust level value, followed by using alarm messages to prevent them from further degrading the network performance.

Our findings are based on the simulation of SZRP to evaluate its performance with respect to the conventional ZRP using NS2 simulator under distinguishable scenarios. The selection of parameters and assumptions for each scenario helps in finding the optimal environment. It shows that SZRP has a minimal adverse impact on packet delay and total routing overhead, while the packet delivery ratio achieved is comparable to

that of ZRP. Thus, our solution is predicted to become applicable for most systems while the lack of slow execution would not be an issue because of the rapid development of processors. The security analyses presented in this thesis emphasize the effectiveness of our secured protocol to provide the required level of security by fulfillment of all security services required by ad-hoc applications such as authentication, integrity, and non-repudiation, and preventing all kinds of attacks threatening ad-hoc networks.

Future Work

Several ideas for future work naturally came up. An enhanced version of SZRP with minor verification will be studied to avoid new attacks that may be performed against this version of SZRP. In addition, a study of the effect of alternative digital signature mechanisms such as elliptic curve can be carried out to reduce the processing time required to perform signing and verification processes.

Finally, an environment with the presence of attackers will be simulated using NS-2 simulator to study the behavior of the current protocols and the enhanced one against all possible attacks.

REFERENCES

[1] A. M. Kamal, “Adaptive Secure Routing in Ad Hoc Mobile Network,” M.S. Thesis, Dept. Computer and Systems Science, Royal Institute of Technology, Stockholm, Sweden, 2004.

[2] Y.-C. Hu and D.B. Johnson, “Implicit source routing in on-demand ad-hoc network routing,” in *Proc.2nd Symposium on Mobile Ad Hoc Networking and Computing MobiHoc*, California, USA, 2001, pp. 1–10.

[3]Yih-Chun Hu, Adrian Perrig, and David B. Johnson. “Ariadne: A Secure On-Demand Routing Protocol for Wireless Ad Hoc Networks”. Wireless Networks, 2005, v.11, pp. 21–38.

[4] C. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector Routing," in *Proc.2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, February 1999, pp. 90-100.

[5] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” in *Proc. Conference on Communications Architectures, Protocols and Applications*, *SIGCOMM*, London, August 1994, pp. 234–244.

[6] Z.J. Haas, M. R. Pearlman, and P. Samer, “The Zone Routing Protocol (ZRP) for Ad Hoc Networks,” Internet Draft, 2003, available at:http://tools.ietf.org/id/draft-ietf-MANETs-zone-zrp-04.txt.

[7] B. Zhu , Z. Wan , M. S. Kankanhalli , F. Bao ,and R. H. Deng, “Anonymous Secure Routing in Mobile Ad-Hoc Networks,” in *Proc. 29th Annual IEEE International Conference on Local Computer Networks*, 2004, New York, pp.102-108.

[8] Y.-C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks”, Ad Hoc Networks, 2003, v.1, pp.175–192.

[9] Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,” *In Proc. ACM Workshop on Wireless Security,* San Diego,WiSe, California, September 2003.

[10] M. G. Zapata and N. Asokan, “Securing Ad Hoc Routing Protocols,” *in Proc. ACM Workshop on Wireless Security* ,Grand Hyatt, WiSe, Singapore, ACM Press, 2002, pp. 1–10.

[11] P. Papadimitratos and Z.J. Haas, “Secure Link State Routing for Mobile Ad Hoc Networks,” in *Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks,* IEEE Press, 2003, pp. 27–31.

[12] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, "A Secure Routing Protocol for Ad hoc Networks," in *Proc. 10th Ann. Int'l Conf. Network Protocols* ,Paris, ICNP, France, Nov.,2002,pp. 78-87.

[13] Y. -C. Hu, A. Perrig, and D. Johnson, "Efficient Security Mechanisms for Routing Protocols," in *Proc. Network and Distributed System Security Symp.,*California, NDPSS , Feb. 2003, pp 57-73.

[14] B. Smith, "Securing Distance-Vector Routing Protocols," M.S. thesis, university of California, California, 1997.

[15] A. A. Pirzada and C. McDonald, "Trust Establishment in Pure Ad-Hoc Networks," Wireless Personal Communications, Vol. 37(1-2), pages 139-168, Springer, 2006.

[16] I. Riedel, "Security in Ad-hoc Networks: Protocols and Elliptic Curve Cryptography on an Embedded Platform," Diploma thesis, Ruhr-Universiät Bochum,Germany, 2003.

[17] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad hoc Networks," in proc*SCS Communication Networks and Distributed Systems Modeling and Simulation Conference ,* San Antonio, CNDPS , TX, January 27-31, 2002.

[18] A.Pirzada, and C. McDonald,"Establishing Trust In Pure Ad-hoc Networks," in *Proc. Twenty-Seventh Australasian Computer Science Conference, Dunedin, New* Zealand, ACSC, 2004, pp 47-54.

[19] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing," IETF Internet Draft, August 2001, available at:http://www.potaroo.net/ietf/idref/draft-guerrero-MANETs-saodv/

[20] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and Secure Source Authentication for Multicast," *in proc. Network and Distributed System Security Symposium,* California, NDPSS ,February 2001, pp. 35–46.

[21] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over LossyChannels,"in*proc. IEEE Symposium on Security and Privacy S&P* ,2000, pp.56-73.

[22] Y. -C. Hu, A. Perrig, and D.B. Johnson. "Packet Leashes:A Defense against Wormhole Attacks in Wireless Ad Hoc Networks". in *Proc. 22nd Ann. Joint Conf. IEEE Computer and communications Societies (INFOCOM 2003),*San Francisco, IEEE Press, 2003, pp. 1976–1986.

[23] L. Qian, N. Song, and X. Li, "Detecting and locating wormhole attacks in Wireless Ad Hoc Networks through statistical analysis of multi-path", in *proc*. *IEEE Wireless Communications and Networking Conference*, *WCNC 2005,* Germany, 2005

[24] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks," Wireless Communications and Mobile Computing (WCMC), vol. 6, issue 4, June 2006, pp. 483-503.

[25] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," in *Proc. ACM Workshop Wireless Security,* Diego, California,*WiSe* , 2003, pp. 30-40.

[26]M. Jakobsson, S. Wetzel, and B. Yener, "Stealth Attacks on Ad-Hoc Networks," in *Proc. of the IEEE Vehicular Technology Conference Fall (VTC-Fall)*,Orlando, Florida, 2003, pp. 2103-2111.

[27] Gupta, V., Krishnamurthy, S. and Faloutsos, M. (2002) "Denial of service attacks at the MAC layer in wireless ad hoc networks", in *Proc. of Military Communications Conference (MILCOM'02)*, Anaheim, CA, USA, pp. 1118-112.

[28] M. Caravaggio. "Understanding Security Issues with Wireless LANs: Security Essentials v1.4b". October 2002. Available at www.giac.org/ practical/maria_caravaggio _GSEC.doc

[29] P. Hanácek, "Problems of Security in Ad Hoc Sensor Network," in *Proc. MOSIS'05,* Ostrava, CZ, MARQ, 2005, pp. 79-84.

[30] P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," in *Proc. IEEE Workshop on Security and Assurance in Ad Hoc Network*s, IEEE Press, 2003, pp. 27–31.

[31] B. Wu, J. Chen, J. Wu, and M. Cardei, "Survey on attacks and countermeasures in mobile ad hoc networks," in *Wireless/mobile network security*, Springer, 2008, ch. 12.

[32] J. Kong, X. Hong, M. Gerla, "A new set of passive routing attacks in mobile ad hoc networks," in IEEE Military Communications Conference, MILCOM 2003, Boston , 2003, pp.796-801

[33] Y. C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security & Privacy, May-June 2004, Volume 2, Issue 3, pp. 28–39.

[34] G. Acs , L. Buttyan ,and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Transactions on Mobile Computing, v.5 n.11, p.1533-1546, November 2006.

[35] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks", in *Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDPS 2002),*San Antonio, Jan. 27-31, 2002.

[36] C. Basile, Z. Kalbarczyk, and R. Iyer, "Neutralization of Error and Attacks in Wireless Ad Hoc Networks," technical report, Univ. of Illinois at Urbana-Champaign, 2005.

[37] K. Fall and K. Varadhan, "Editors ns Notes and Documentation," The VINT Project, UC Berkeley, LBL, USC/ISI, and Xerox PARC, November 1997. Available from http://www-mash.cs.berkeley.edu/ns

[38] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," *in Proc. 7th International Workshop*, Berlin Heidelberg, 1999, pp171–178.

[39]S. Čapkun, J.-P. Hubaux, and L. Buttyán, "Mobility Helps Security in Ad Hoc Networks," in *Proc. ACM Int'l Symp Mobile Ad Hoc Networking and Computing,* Annapolis, 2003, pp46-56.

[40]V. D. Gligor, "Security of emergent properties in ad-hoc networks," in *Proc. International Workshop on Security Protocols*, Cambridge, UK, Apr. 2004.

[41]V. Gligor, "Handling new adversaries in secure mobile ad-hoc networks," in *Proc. ESNS2007*,California, 2007.

[42] W. Kozama and L. Lazos "REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits", *In Proc. 2nd ACM conference on Wireless Network Security, WiSec'09*, Zurich, Switzerland, 2009.

[43] I. D. Chakeres and E. M. Belding-Royer, "AODV Routing Protocol Implementation Design," *in Proc. the International Workshop on Wireless Ad hoc Networking (WWAN), Tokyo, Japan, March 2004,* pp698-703.

[44]S.R. Das, C.E. Perkins and E.M. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks," in *Proc. of INFOCOM 2000*, Tel-Aviv, Israel ,March 2000,pp. 3-12.

[45] F. Kargl, S. Schlott, A. Klenk, A. Geiss, A. and M. Weber, "Securing Ad hoc Routing Protocols," in *Proc. 30th Euromicro Conference, Rennes* , France,2004, pp514-519

[46] Sh. Rahmatizadeh**,** H. Shah-Hosseiniand H. Torkaman "The Ant-Bee Routing Algorithm: A New Agent Based Nature-Inspired Routing Algorithm", Journal of Applied Sciences, 2009, Volume 9, Issue 5, pp. 983–987.

[47] H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE communication magazine, 2002, pp. 70-75.

[48] Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing,"IEEE Security & Privacy, 2004, pp 24-39.

[49] H. Nguyen, U. Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks,"Ad Hoc Networks, 2008, v.6, pp. 32–46

[50] M. Poturalski, P. Papadimitratos, and J. Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility", in *Proc. ACM Symposium on Information, Computer & Communication Security ASIACCS* '08, Tokyo, Japan, 2008.

[51] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, J. Hubaux, "Secure neighborhood discovery: a fundamental element for mobile ad hoc networking," *IEEE communication magazine*, 2008, V. 46, Issue: 2, pp. 132-139

[52] Y. Xioa, X. Shen, and D. Du, "Secure routing in wireless ad-hoc networks," in *Wireless Network Security,* New York, Springer Science and Business Media, 2007, ch. 6, pp. 137-158.

[53]W. Stallings, "Cryptography and network security principles and practices," 4th edition, Prentice Hall, 2005.

[55] Statistical Package for the Social Sciences: SPSS for Windows, Rel. 10.0.0. 1999. Chicago: SPSS Inc., available at: http://spss.en.softonic.com.

[56] B. Wu., J. Wu, E. B. Fernandez, M. Ilyas, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks " *Journal of Network and Computer Applications*, 2007, Springer, Volume 30, pp. 937–954.

[57] B. Forouzan, "Introduction to cryptography and network security," McGraw-Hill, 1st ed., 2006.

[58] R Poovendran, L Lazos, "A Graph Theoretic Framework for Preventing the Wormhole Attack in Wireless Ad Hoc Networks," *Wireless Networks*, 2007, Springer

[59]Y. Zhang, W. Lou, W. Liu, "A secure incentive protocol for mobile ad hoc networks," *Wireless Network*, 2007, volume 13, pp. 569–582.

[60] M. Rafsanjani and A. Movaghar, "Identifying Monitoring Nodes with Selection of Authorized Nodes in Mobile Ad Hoc Networks," *World Applied Sciences Journal*, 2008, vol. 4, pp. 444-449.

[61] R. Lambert. (2006, Jan 18). *Understanding elliptic-curve cryptography*, Available: http://www.eetimes.com/design

[62] M Poturalski, P. Papadimitratos, and J. Hubaux. "Secure Neighbor Discovery in Wireless Networks" ", *In Proceedings of the 2008 ACM symposium on Information, computer and communications security,* Tokyo, Japan, 2008.

[63]S. Cheung and K. Levitt, "Protecting routing infrastructures from denial of service using cooperative intrusion detection", *In Proceedings of the 1997 New Security Paradigms Workshop* (September 1998) pp. 94–106.

[64] R. Pickholtz, D. Schilling, and L.B. Milstein,"*Theory of spread spectrumcommunications—a tutorial,*" IEEE Transactionson Communications, v.5 n.30,p. 855–884, 1982.

[65] J. Schaumann, (2002),"Analysis of the Zone Routing Protocol",Available at:http://www.netmeister.org/misc/zrp/zrp.htm

[66] Z.J. Haas, M. R. Pearlman, and P. Samer, "Intrazone Routing Protocol (IARP)," Internet Draft, 2001, available at:http://tools.ietf.org/id/draft-ietf-MANETs-iarp-01.txt.

[67] Z.J. Haas, M. R. Pearlman, and P. Samer, "Interzone Routing Protocol (IERP)," Internet Draft, 2001, available at:http://tools.ietf.org/id/draft-ietf-MANETs-ierp-01.txt.

[68] Z.J. Haas, M. R. Pearlman, and P. Samer, "The Bordercast Resolution Protocol (BRP)," Internet Draft, 2001, available at:http://tools.ietf.org/id/draft-ietf-MANETs-brp-01.txt.

[69] G. Montenegro and C. Castelluccia, "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses", presented at Network and Distributed System Security Symposium, NDPSS '02, San Diego, California, February 2002.

[70] k. Kang, D. Kim, T. Kwon, and J. R. Choi, "An efficient implementation of hash function processor for IPSec",*In Proceedings of the 2002 IEEE Asia-Pacific*,Taipei, Taiwan, August. 2002, pp. 93-96