SECURE PARTIALLY SPATIAL DISJOINT MULTIPATH ROUTING PROTOCOL OVER MANETS

By
Roba Khaled Mohammad Al-Soub

Supervisor
Dr. Wesam A. AlMobaideen

Co-Supervisor
Dr. Azzam T. Sliet

This Thesis was Submitted in Partial Fulfilment of the Requirement for the Master's Degree of Computer Science

Faculty of Graduate Studies
The University of Jordan

January, 2008

COMMITTEE DECISION

This Thesis/Dissertation (Secure-Partially Spatial Disjoint Multipath Routing Protocol over MANETs) was Successfully Defended and Approved on 22-12-2008

Examination committee	**Signature**
Dr. Wesam A. AlMobaideen (Supervisor) Associate Prof. in Computer Networks	....
Dr. Azzam T. Sliet (Co-Supervsior) Associate Prof. of Spatial Database	....
Dr. Mohammad S. Qatawneh (Member) Associate Prof. in Parallel Systems and Networks	....
Dr. Imad K. Salah (Member) Associate Prof of Complex Systems and Networks	....
Dr. Mohammad Al-Abbadi (Member) Assistant Prof. of Image Processing Mu'tah University	....

DEDICATIONS

To the soul of my late grandmother whom I missed her compassion and
prayers, I hoped she was with me now to see the happiness in her eyes while
I am finishing this work.

To my inspiring in life, the symbol of challenge and hard working..
The one who taught me determination and persistence..
The one who granted me the courage and the strength,
the truth and the generosity...
To my dear father.

To the resource of peace and sympathy…
To the brightness in the darkness…
To the one who granted me love without tiredness..
To the one who prays for me every night…
To the pure heart… My darling mother.

To the candle that enlightened my life with hope..
To the one who covered me with love…
The one who always encouraged and supported me
without waiting awardness ....
To my dearest aunt.

To the rosy part of my life, my dearest brother, Ahmad and my darling
sisters, Hadeel, Kida'a, Ghadeer, Nadia, Bara'ah,
who always supported me with their love and compassion.

To those who lived the experience with me...
Who helped me make the difficult easy..
Who stood beside me all the times with their
love, advice and support ....To my friends especially
Shefa'a, Amal, and Wala'a.

To all, I dedicate this work.

ACKNOWLEDGMENT

Writing the last words of my thesis is very beautiful moment which reflects all memories in my journey during writing this thesis. Every moment has been spent accomplishing this work was full of knowledge and experiences mixed with hope, tears and tension. In this regard, I humbly thank Allah for his Almighty and Mercy, who inspired my soul with patience and granted me health, thoughts and co-operative people to enable me achieve my goal.

Thanks to all who worked hard and succeeded in spreading knowledge and ethics…To all who have the sense of responsibility toward their students to enlighten their ways…To my teachers. My deep thanks are extended to my supervisor, Dr. Wesam AlMobaideen for his continuous support, creative ideas, sincere advises and even harsh criticisms which were a constant resource of inspiration for me. I will never forget his motivating advice not only regarding this thesis, but also concerning my ambitions for the future. I admit that without his efforts and support, this work would never appear in its final shape. Thanks for Dr. AlMobaideen since he always wants the best for me and pushes me forward to do it. I would like also to thank Dr. Azzam Sliet, my co-supervisor, for his guidance, valuable comments and helpful suggestions which were a great motivation for me. Thanks for his effort and continuous assist that helped me accomplish this work.

Further more, I would like to present my deep gratitude to Dr. Mohammad Qatwneh for his unlimited support and encouragement during the course of my study. I am also profoundly grateful to my uncle Dr. Fayez Al-Soub for his motivation and valuable help during the review of this thesis.

Finally, I want to thank my family; my parents, my aunt and uncles, my brother and sisters for their maintain support and prayers which acted as an effective point in my academic life.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AEADMRA	Ant-based Energy Aware Disjoint Multipath Routing Algorithm
AODV	Ad hoc On-demand Distance Vector Routing
AOMDV	Ad hoc On-demand Multipath Distance Vector
AP	Access Point
BSS	Basic Service Set
CA	Certificate Authority
CBR	Constant Bit Rate
CSMA	Carrier Sense Multiple Access
DCF	Distributed Co-ordination Function
DoF	Denial of Service
DSDV	Destination Sequenced Distance Vector Routing
DSR	Dynamic Source Routing
FSR	Fisheye State Routing
GEANDMRA	Grid-based Energy Aware Node-Disjoint Multipath Routing Algorithm
GloMoSim	Global Mobile information system Simulation library
HARP	Hybrid Ad hoc Routing Protocol
IR	Improvement Ratio
MAC	Message Authentication Code (MAC)
MAC-layer	Medium Access Control
MANET	Mobile Ad hoc Network
MP-SAR	Multi-Path Security Aware Routing
MSDMP	Maximally Spatial Disjoint Multipath Routing Protocol
MWNs	Multi-Hop Wireless Networks

M-Zon	Multiple Zones-based Routing Protocol
NDMR	Node-Disjoint Multipath Routing Protocol
PHR-AODV	Path Hopping Reverse AODV,
R-AODV	Reverse-AODV
RREP	Route Replay
RREQ	Route Request
SAODV	Secure Ad hoc On-demand Distance Vector
SAR	Security Aware Routing
SDMP	Secured Data based Multipath Routing Protocol
SDMSR	Secure, Disjoint, Multipath Source Routing Protocol
SEAD	Secure Efficient Ad hoc Distance Vector Routing
SecMr	Secure Multipath Routing Protocol for Ad hoc Networks
SMR	Split Multipath Routing
SMS	Shortest Multipath Source Routing
S-MSDMP	Secure-Maximally Spatial Disjoint Multipath Routing Protocol
S-PSDMP	Secure-Partially Spatial Disjoint Multipath Routing Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network
WRP	Wireless Routing Protocol
ZRP	Zone Routing Protocol

SECURE PARTIALLY SPATIAL DISJOINT MULTIPATH ROUTING PROTOCOL OVER MANETS

By
Roba Khaled Mohammad Al-Soub

Supervisor
Dr. Wesam A. AlMobaideen

Co-Supervisor
Dr. Azzam T. Sliet

ABSTRACT

In the last few years, there has been a growing interest in Mobile Ad hoc Networks (MANET) due to its wide applications. Routing in MANETs is challenging task and several routing protocols have been proposed to give solutions of the problems emerged in MANET. Reactive (on-demand) routing protocols are a kind of routing protocols used in MANET. Multipath routing is one of the most significant research directions in the area of network routing. Recent research has started to focus on multipath routing protocols to obtain better reliability, fault tolerance and load balancing in varying network conditions.

With the increasing interest in MANETs, there has been a great focus on the security issues in such networks. Several researches exist, which try to design a secure routing protocol for ad hoc networks, in order to offer protection against specific attacks or sets of attacks. In this thesis we introduce the Secure- Partially Spatially Disjoint Multipath (S-PSDMP) routing protocol, as a security extension to the Maximally Spatially Disjoint Multipath (MSDMP) routing protocol. S-PSDMP chooses the most spatially disjoint paths which could join partially via nodes that specify certain security threshold.

Simulation results show that S-PSDMP increases the network throughput and reduces both the amount of discovery overhead and end-to-end delay as compared with Secure-Maximally Spatially Disjoint Multipath (S-MSDMP) routing protocol. The average improvement ratio of throughput is 2%, and the average improvement ratio of end-to-end delay and discovery overhead reduction are 5% and 14% respectively.

1. INTRODUCTION

1. Introduction

1.1 Overview:

Nowadays there is a growing demand on wireless networks for their ease of use, ease of deployment and low cost. A wireless network is a technology that enables users to be connected and to communicate without being linked to a wired network. Wireless local area networks (WLANs) were developed as a mean to provide high bandwidth to users in a limited geographical area. Wireless networks fall into one of two widely known communication modes; the infrastructure mode or infrastructure-less mode which is totally wireless and called mobile ad hoc networks (MANET). In the case of infrastructure, WLAN the network is divided into cells called Basic Service Set (BSS). Each cell is controlled by an Access Point (AP), which provides the communication between the mobile nodes in the cell and other wired and wireless networks (Crow et al, 1997).

Figure 1.1 shows a sketch of infrastructure network.

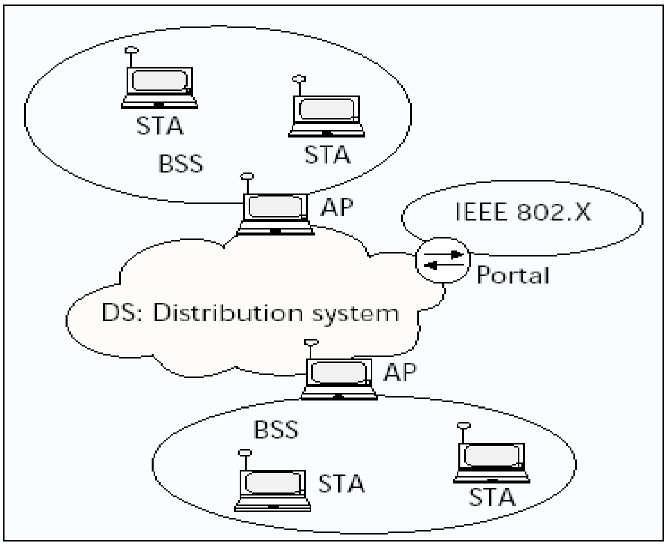


Figure 1.1: A sketch of infrastructure network (Crow et al, 1997)

For the Mobile ad hoc networks (MANET's), the network is composed of a collection of dynamic mobile nodes which are self organized, and able to communicate without using a network infrastructure. The need for ad hoc networks emerges in situations where fixed network infrastructure cannot exist or has been destroyed (Heide Clausen et al, 2002).

In MANET's the network topology is very dynamic due to the node mobility over the time. Each mobile node has a limited radio power that represents its transmission range. Figure 1.2 shows a sketch of an ad hoc network (Crow et al, 1997).

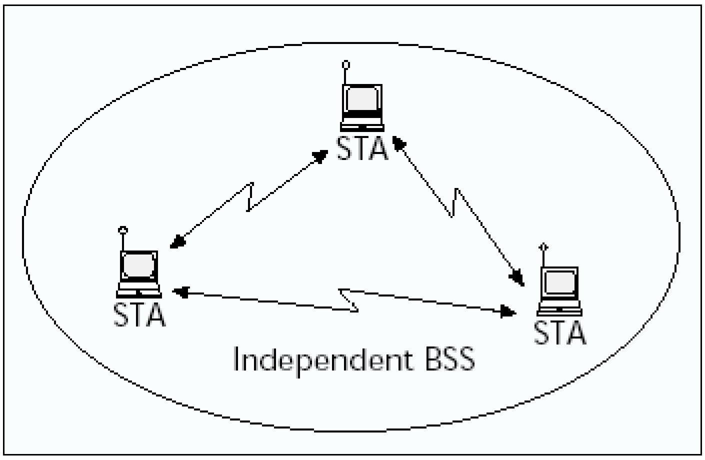


Figure 1.2: A sketch of infrastructure-less network (Crow et al, 1997)

The limited transmission range restricts the node to communicate directly only with the nodes that reside within its transmission range. However, if a node sends data to another one outside its transmission range, then sender will use other intermediate nodes to reach the destination. Therefore, each node in an ad hoc network acts as a mobile host and as a router to guarantee end-to-end packet delivery.

1.2 MANET Properties

In the last few years, there has been a growing interest in ad hoc networks due to its wide applications. Some of these applications are disaster areas, military applications, business and meeting rooms, airports, distance learning, and even for networks in building where cabling configurations are difficult .The following point illustrates some of MANET's properties that differentiate it from the traditional wired network in many aspects (Crow et al, 1997) and (IEEE 802.11, 2007).

- Limited Bandwidth: This important feature affects the nodes and the network lifetime. For wired network, the available Bit rates are 1,000 Mbit/s, while a limited data rates are offered with wireless networks.
- No infrastructure is provided: All the participating nodes in the wireless networks act as a router and responsible of forwarding network traffic to other nodes.
- User Mobility: Since wireless networks enable nodes to move freely in the environment, a continuous breaking and rebuilding of link in the network makes the network topology vary over time.
- Power Consumption is an important factor in wireless networks since battery limitation affects the power of the signals used in the transmission operations known as the radio range.
- Throughput: The capacity of WLANs should ideally be close to that of wired networks. However, the physical limitations and limited available bandwidth make WLANs operate at data rates between 1–20 Mb/s.

- Security: The lack of infrastructures in wireless network makes it vulnerable to many types of attacks. In a wired network, the transmission medium can be physically secured, and access to the network is easily controlled. However, with wireless network this is more difficult to secure due to the fact that transmission medium is open to anyone within the geographical range of a transmitter. Data privacy is usually accomplished over a radio medium using encryption. While encryption of wireless traffic can be achieved, it is usually at the expense of increased cost and decreased performance.

Active research work for mobile ad hoc network focuses, mainly, on the fields of medium access control, routing, resource management, power control and security. As we notice, the scarce resources in MANET's such as power consumption, computational capabilities, and low communications bandwidth make the design of routing protocols as a key challenge, and an intelligent routing strategy is needed to overcome these problems (Abolhasan et al, 2004) and (Heide Clausen et al, 2002).

1.3 Routing in MANET

Routing is a fundamental issue of networks. A lot of mobile ad hoc network routing protocols have been proposed in the last few years to address the problems associated with routing in MANET's. There are some challenges that make the design of mobile ad hoc network routing protocols a difficult task. Firstly, in mobile ad hoc networks, node mobility causes frequent topology changes and network partitions. Secondly, because of the variable and unpredictable capacity of wireless links, packet losses may happen frequently. Moreover, the broadcast nature of wireless medium introduces the hidden terminal and the exposed terminal problems. Additionally, mobile nodes have restricted power, computing and bandwidth resources and require effective routing schemes (Liu and Kaiser, 2005).

The principal objective of a routing protocol is efficient discovery and establishment of a route between the source and the destination so that there can be an efficient delivery of information between them. Many routing protocols have been proposed to solve the problems emerged in MANET. These protocols are generally classified based on how routing information is acquired and maintained by mobile nodes. Using this method, mobile ad hoc network routing protocols can be divided into proactive (table-driven) routing, reactive (on-demand) routing, and hybrid routing (Royer and Toh, 1999) as shown in Figure 1.3.

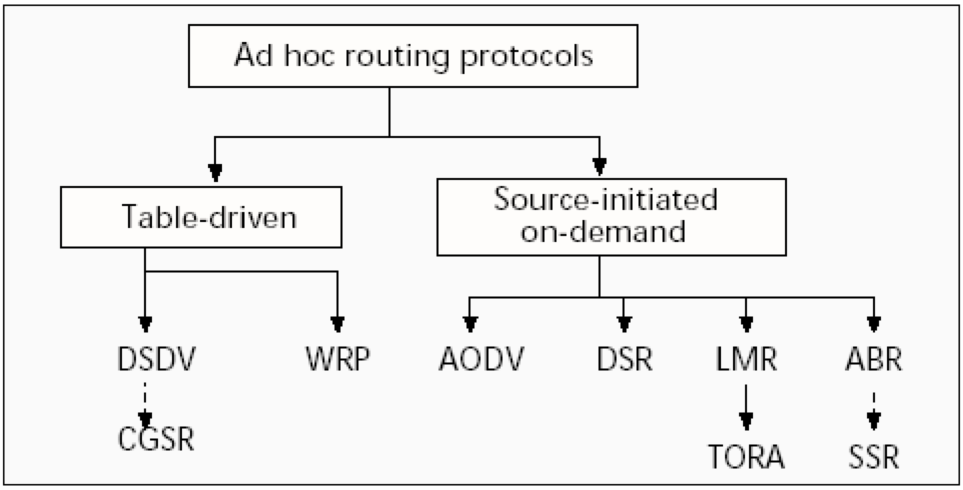


Figure 1.3 Categorization of ad hoc routing protocols (Royer and Toh, 1999)

By using a proactive routing protocol, each node continuously maintains routing information to all other nodes in the network (or parts of the network) through periodic update process. In proactive routing, each node in the network attempts to maintain consistent up-to-date routing information. Thus, a source node can get a routing path immediately if it needs one. Using proactive routing algorithms, mobile nodes proactively update network state and keep a route regardless of whether data traffic exists or not, and the overhead to maintain up-to-date network topology information is high. Destination Sequenced Distance Vector routing (DSDV), Wireless Routing Protocol (WRP), and the Fisheye State Routing (FSR) are examples of protocols based on proactive approach (Liu and Kaiser, 2005).

Reactive routing protocols were designed to reduce the overheads incurred in proactive protocols by maintaining information for active routes only. With on-demand, routing each node maintains routing information only when it requires sending data to a particular destination. Route discovery usually occurs by flooding a route request packets through the network. The route discovery is completed if either a route is founded or all possible route permutations have been examined (Royer and Toh, 1999).

Compared to the proactive routing protocols, less control overhead is a distinct advantage of the reactive routing protocols. Thus, reactive routing protocols have better scalability than proactive routing protocols in mobile ad hoc networks. However, when using reactive routing protocols, source nodes may suffer from long delays for route searching before they can forward data packets. Examples of protocol based on reactive routing are the Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector Routing (AODV) (Abolhasan et al, 2004).

Hybrid routing protocols are proposed to combine the features of both proactive and reactive routing protocols and overcome their shortcomings. Normally, hybrid routing protocols for mobile ad hoc networks exploit hierarchical network architectures.

Proper proactive routing approach and reactive routing approach are utilized in different hierarchical levels, respectively. Examples of such protocols are the Zone Routing Protocol (ZRP) and Hybrid Ad hoc Routing Protocol (HARP) (Liu and Kaiser, 2005).

Ad hoc routing protocols can be divided into single path routing and multipath routing according to the number of discovered paths between source and destination pairs. Multipath routing is preferred to reduce both the latency of discovering a new route after a link breakage and the control overheads since route discovery is needed only when all the discovered paths fail. Depending on the participating nodes (or links) in the path between two end nodes, multipath routing protocols can be node-disjoint or link-disjoint (Marina and Das, 2001).

Most of the existing multipath routing protocols are either multipath extensions of Ad hoc On-demand Distance Vector (AODV) (Perkins and Royer, 1999), or Dynamic Source Routing (DSR) (Johnson and Maltz, 1996). Most of these protocols are typical protocols used to find disjoint paths but they can hardly find node-disjoint multiple paths in large-scale networks efficiently.

1.4 Security over MANET's

Security is an important issue in MANET's. The provision of security services in the MANET context faces a set of challenges, which do not appear in wired networks. No centrally administered secure routers, no strict security policies, the highly dynamic nature of mobile ad hoc networks, also the broadcast nature of the nodes and the absence of fixed infrastructure make the network vulnerable to many types of attack (Mavropodi and Douligeris, 2006).

Ad hoc networks are exposed to many possible attacks. These attacks can be classified to passive attacks and active attacks. In passive attacks, attackers do not disturbs the operation of routing protocol but only attempt to detect valuable information by listening to the routing traffic. Defending against such attacks is difficult because it is usually impossible to detect eavesdropping in a wireless environment. While in active attack, attackers inject arbitrary packets and try to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes (BOUAM and BEN-OTHMAN, 2003).

There are specific types of attack that can appear in MANET's such as:

- Black hole attack: An attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it.
- Replay attack: An attacker sends old advertisements to a node causing it to update its routing table with stale routes.
- Wormhole attack: An attacker records packets at one location in the network, and tunnels them to another location, routing can be disrupted when only routing control messages are tunnelled.
- Denial of Service (DoF) attacks: Denial of service attacks aim at the complete disruption of the routing function and therefore the whole operation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture (Argyroudis and O'Mahony, 2004).
- Lack of cooperation: This type of attack happens when the node does not provide its services to other nodes to save its own resources like, computation power and energy. (Berton et al, 2006).

To solve the security problems in an ad hoc network and make it secure, there are a number of requirements that have to be taken into account, as described below (Zhou and Haas, 1999).

- Availability: the network must be available all the time to enable all nodes in the network send and receive messages despite of network being under attack. An attack can be in the form of a denial of service. Or, if an attacker disrupts the routing protocol or some other high-level service and tries to disconnect the network. The node itself can make a problem with the availability.
- Confidentiality: provides privacy to sensitive data being transmitted over the network. This requirement is important especially in military uses where strategic and tactical information is sent across the network. If an adversary takes this information, it may have disturbing consequences.
- Integrity: ensures that messages being sent over the network are not corrupted.
- Authentication: the function of authentication service is to ensure the destination that the received message is from the source it claims to. The authentication assures the node identity in the network.
- Non-repudiation: prevent either the source of a message or the destination from denying transmitted message. The sender cannot deny having sent the message and are therefore responsible for its contents. Non-repudiation is particularly useful for detection of compromised nodes.

In mobile ad hoc networks, security depends on several parameters as mentioned above and concerns two aspects: routing security and data security. These aspects are subject to many vulnerabilities and attacks. Nodes are easier to be stolen since they are mobile and the computing capacity is limited. Also, ad hoc networks services are provisional and batteries are limited that makes a Denial of Service attack, by consumption of energy, very possible (BOUAM and BEN-OTHMAN, 2003).

Most of the widely used ad hoc routing protocols have no security considerations and they are cooperative by nature. The existing routing protocols implicitly trust all the participants to forward routing and data traffic. This assumption can prove to be terrible for an ad hoc network that relies on intermediate nodes for packet forwarding. This naive trust model allows malicious nodes to disrupt an ad hoc network by inserting incorrect routing updates, replaying old routing information, changing routing updates, or advertising incorrect routing information (Han et al, 2006) and (Argyroudis and O'Mahony, 2004).

There are several proposals that try to design a secure routing protocol for ad hoc networks, in order to offer protection against the attacks mentioned above. These proposed solutions are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing ones (like DSR and AODV). A common design principle in all the studied proposals is the performance-security trade-off balance. Since routing is an essential function of ad hoc networks, the additional security solutions should not obstruct its operation (Argyroudis and O'Mahony, 2004).

Several solutions for secure routing have been proposed but they cannot solve the problems that arise in multipath routing since they are designed for single path routing protocols (Mavropodi and Douligeris, 2006).

Security over multipath routing protocols has not been widely deployed over ad hoc wireless networks. Most of the researches focused on the networks functionality and efficiency issues with less concern of security issues (Mavropodi and Douligeris, 2006). Secure multipath routing protocol for ad hoc networks (SecMR) is an example of such protocol (Mavropodi et al, 2007).

1.5 Motivations and Objectives

In this thesis, we are interested in multipath routing protocol, such as Ad hoc On-demand Multipath Distance Vector (AOMDV) protocol, and the potential security improvement that could be achieved by choosing the most secure spatially separated node-disjoint paths, which could partially join via nodes that specify certain security threshold. Due to the importance of security in MANET's, this study tries to find trade-off between efficient routing and the security measurements in the network. This study aims to increase the network performance in terms of throughput and security -by transmit data using trusted nodes- and at the same time to reduce both discovery overhead and average end-to-end delay.

In this study, we propose the Secure-Partially Spatial Disjoint Multipath routing protocol (S-PSDMP). S-PSDMP, is a modification to MSDMP (Almobaideen et al, 2008), chooses the most spatially disjoint paths, which could join partially via nodes that specify certain security threshold. We believe that allowing partially disjoint paths that are most secure could be better than choosing other maximally spatially disjoint paths that are less secure.

In S-PSDMP, choosing the secure spatially disjoint paths receives the improvement obtained by MSDMP with taking security measures into estimate. MSDMP sends data using spatial separated path and it is proven that sending data packet in this way will increase the network performance by minimizing the probability of collision between nodes send data on different paths. S-PSDMP transmits data on less number of paths than MSDMP but S-PSDMP chooses trusted nodes to participate in data transmission, which in turn ensures that the transmitted data passed through secured nodes.

The objective of this thesis is to study the proposed S-MSDMP and whether the security enhancement affects the network performance obtained by MSDMP. We will study the impact of S-PSDMP on the average end-to-end delay, routing overhead, and the overall network throughput. The results of S-PSDMP will be compared with the result of Secure-MSDMP (S-MSDMP).

In the literatures we review, there have been several protocols that present solutions for security over multipath routing in ad hoc networks. In this thesis, we go over some of these solutions.

1.6 Thesis Organization

This thesis contains five chapters outlined as follows:

Chapter one: presents a brief introduction about wireless networks and their properties, Routing in MANET, and addresses a security issues over MANET’s. It also highlights the main objectives of the study.

Chapter two: presents the multipath routing protocols and some security issues. Some common secure routing protocols for ad hoc networks are also reviewed.

Chapter three: introduces the proposed S-PSDMP.

Chapter four: presents detailed description of simulation environment and the results obtained from the simulation. This chapter also gives an introduction about the GloMoSim network simulator.

Chapter five, finally conclusion of the thesis with future work.

LITERATURE REVIEW

2. Literature Review

2.1 Introduction

This chapter sheds light over some related work to routing protocols in MANET's. We begin with an introduction to the multipath routing in MANET's and next an overview of both the Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol and the Maximally Spatial Disjoint Multipath (MSDMP) routing protocol.

2. 2 Multipath Routing in MANET's

Recent research has focused on multi path routing protocols for fault tolerance and load balancing. Multipath on-demand routing protocols try to discover multiple paths at both the traffic sources and at intermediate nodes in a single route discovery attempt. This reduces both the route discovery latency and the control overheads since the route discovery is needed only when all the discovered paths fail. Scattering the traffic along several paths make the probability of congestion and bottlenecks low. Multipath routing also provides a higher bandwidth and effective load balancing since the load of data forwarding can be distributed over the existing paths (Meghanathan, 2007).

Although various benefits have been explored for multipath routing in MANET's, not all these advantage utilized because the traffic along different paths may interfere with each other due to the broadcast nature of radio transmission. Also the multiple paths are utilized as a backup or auxiliary method in most of multipath routing protocols (Wu and Harms, 2001).

Depending on the participating nodes (or links) in the path between two end nodes, multipath routing protocols can be node-disjoint or link-disjoint. For a particular source S, and destination D, the set of node-disjoint routes consists of paths that do not have nodes present in more than one of S-D path (except the source and destination). Similarly, the set of link-disjoint path consist of paths that do not have certain link present in more than one of S-D path.

Most of the existing multipath routing protocols are either multipath extensions of Ad hoc On-demand Distance Vector (AODV) (Chakeres and Belding-Royer, 2004), or Dynamic Source Routing(DSR) (Johnson and Maltz, 1996). Ad hoc On-demand Multipath Distance Vector Routing (AOMDV) is a multipath extension of AODV that computes multiple loop-free link-disjoint routes (Marina and Das, 2001). Split Multi-path Routing (SMR) is a multipath routing protocol that modifies DSR by finding the set of maximally node-disjoint path between a source and destination (Lee and Gerla, 2001). In this study, we are interested in on-demand multipath routing protocol, such as Ad hoc On-demand Multipath Distance Vector (AOMDV) protocol (Marina and Das,2001), and the security improvement that may be achieved through the modifications we propose.

The Ad Hoc On-demand Distance Vector Routing (AODV) protocol (Perkins and Royer, 1999) is a reactive routing protocol for mobile ad hoc networks. As a reactive routing protocol, AODV maintain information when routes needed only. The AODV builds a single loop free path to each other node on the network. In AODV, only one path is saved although extra packets are sufficient to construct more than one path. The advantage of AODV is that it is adaptable to highly dynamic networks. However, a node may experience large delays during route construction, and link failure may initiate another route discovery, which introduces extra delays and consumes more bandwidth (Perkins and Royer, 1999).

2.2.1 AOMDV Overview

The ad hoc on-demand multipath distance vector (AOMDV) routing protocol extends the AODV algorithm to build and store several paths in the routing table. In AMODV when one route to a destination is broken, it does not necessarily result to a new route discovery. Instead, the source node can simply select the next available route from the table (Marina and Das, 2001).

In AOMDV, each node has a routing table keeps routing information for the destination to which it currently has a route. Periodic hello messages may be used to detect and monitor links to neighbors and to update the routing table. A routing table entry expires if it has not been used or reactivated for a pre-specified expiration time. Moreover, AOMDV adopts the destination sequence number technique used by AODV combined with a new notation of advertised hop count to guarantee loop freedom (Marina and Das, 2001)

When a traffic source needs a route to a destination in AOMDV, it starts route discovery process. Route discovery process initiated by flooding Route Request (RREQ) packet across the network and waiting for Route Reply (RREP) message. Any intermediate node receiving a RREQ sets up a reverse path to the source, and if it has a valid route to the destination it will generate RREP, otherwise it will rebroadcast the

RREQ packet. When destination node receives a RREQ, it also generates a RREP. The generated RREP will be sent directly to the source using the reverse path.

AOMDV RREQ Message

A source node initiates the RREQ when it has a data packet to be sent to a specific destination. Figure 2.1 shows the structure of the RREQ packet used in AOMDV. The fields of RREQ are described below.

<table>
<tr><td>Type</td><td>Flags</td><td>Hop Count</td></tr>
<tr><td colspan="3">Last Address</td></tr>
<tr><td colspan="3">Next to Last Address</td></tr>
<tr><td colspan="3">Broadcast ID</td></tr>
<tr><td colspan="3">Destination Address</td></tr>
<tr><td colspan="3">Destination Sequence Number</td></tr>
<tr><td colspan="3">Originator Address</td></tr>
<tr><td colspan="3">Originator Sequence Number</td></tr>
</table>

Figure 2.1: AOMDV RREQ Message Format (Zeng et al, 1998).

- Type: the type of the packet, which equals 1 for RREQ.
- Flags: some flags for special use of RREQ such as gratuitousRREP, destinationOnly; and unknownSeqNo flags.
- Last Address: stores the address of the node that forward the RREQ packet.
- Next to Last Address: stores the address of the node that receives the RREQ after the source (this node will be the last one before the source in the reverse path from the destination).
- Broadcast ID: the RREQ ID, used with source address as a primary key to identify a specific RREQ.
- Destination Address: the address of the end destination.

- Destination Sequence Number: the last saved sequence number of the end destination.
- Originator Address: the address of the node that initiates the RREQ to the destination.
- Originator Sequence Number: the current sequence number of the source node of the RREQ.

2.2.2 MSDMP Overview

MSDMP modifies the ad hoc On-Demand Multipath Distance Victor routing protocol (AOMDV) (Marina and Das, 2001) to discover a set of node-disjoint paths, which are spatially separated. In order to achieve the spatiality and the node disjointness property, MSDMP modifies the structure of AOMDV Route Request (RREQ) message and adds two new tables, (Almobaideen et al, 2008). These tables and the new structure of the RREQ are described below. The words message and packet will be used interchangeably through the rest of this thesis.

MSDMP RREQ Message

The MSDMP modifies the AOMDV RREQ message to include the list of node participating in the path between a specific source and destination. The list of path included in the RREQ message helps in deciding whether a specific route satisfies the disjointness property or not. Figure 2.2 shows the new RREQ message used in MSDMP. As shown in the figure the new filed added to the RREQ message is the Route List field, which stores the addresses of the nodes that are participated in the path.

Type	Flags	Hop Count
Last Address		
Next to Last Address		
Broadcast ID		
Destination Address		
Destination Sequence Number		
Originator Address		
Originator Sequence Number		
Route List		

Figure 2.2: MSDMP RREQ Message Format (Almobaideen et al, 2008)

MSDMP Tables

MSDMP utilizes additional two tables for proper operation. The first table is the Seen RREQ Table in which a node inserts information about the RREQ it handles. The second table is the Replied RREQ table. The node that generates a Route Reply (RREP) message to record the information about the route used in this reply uses this table.

Seen RREQ Table:

In this table any node handles a RREQ packet inserts information about the RREQ in a table entry. The node uses the stored information to assure that the RREQ will not be processed again. Following is a description of the field of this table (Almobaideen et al, 2008).

- Broadcast Id: the RREQ ID used to define the RREQ message.
- Source Address: the address of the initiate the RREQ message.
- First after Source: the first node that gets the RREQ packet from the source.

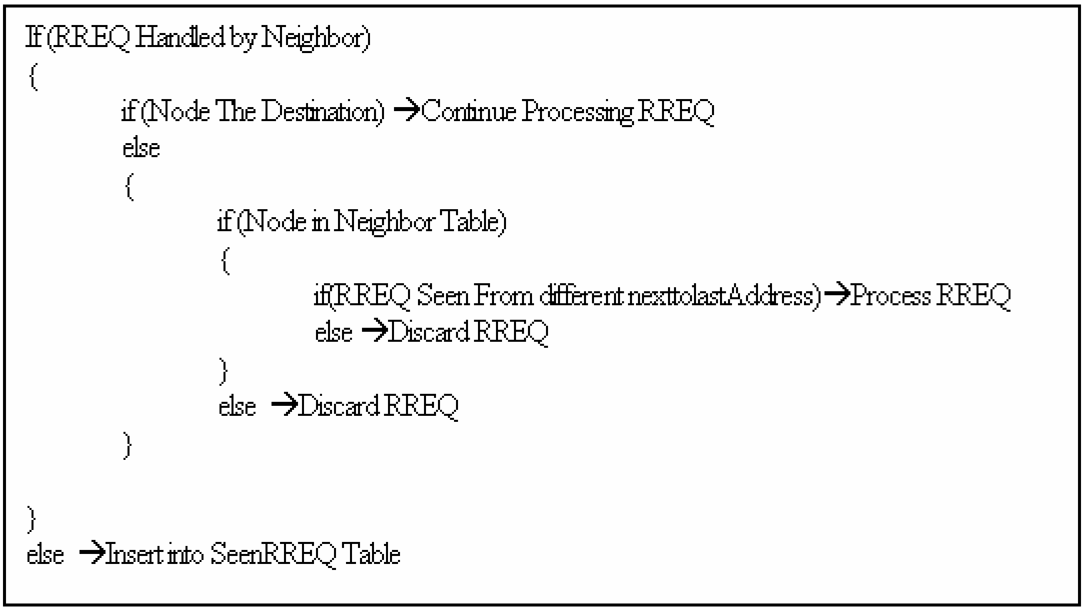
Replied RREQ Table:

This table contains information about the RREQ packets, which have been replied by a certain node. The table stores the route path used in each reply to enable the node in deciding if a new path is node disjoint path or not. The field of this table is described below (Almobaideen et al, 2008).

- Broadcast Id: the RREQ ID, used to define the RREQ message.
- Source Address: the address of the node that initiates the RREQ message.
- Last before Source: the same as (First after Source) described in the table above, but it is called (Last before Source) because we are dealing with the reverse path in this table.
- Next Hop: the fist node after the node that generates the RREP.
- Route List: the list of nodes that participate in a specific node disjoint multipath between a source and a destination.

Operational Description of MSDMP

The objective of MSDMP is to find the set of paths that are spatially separated and maximally disjoint. MSDMP design is based on AOMDV (Marina and Das, 2001). When a traffic source needs a route to specific destination, it starts route discovery process. Route discovery process is initiated by flooding RREQ packet across the network and waiting for RREP. Any intermediate node receiving a RREQ checks the Seen RREQ table to see if this RREQ is processed before. If yes, it will not process this route request unless if it is the first node after source or the last node before destination. Figure 2.3 presents the algorithm used by MSDMP. Any node decides to rebroadcast the RREQ must add its own address in Route-List in the RREQ. The reason of allowing the nodes after source and before destination to process more than one RREQ is to allow the protocol to discover as many as existed spatially separated path (Almobaideen et al, 2008).



```
If (RREQ Handled by Neighbor)
{
        if (Node The Destination) →Continue Processing RREQ
        else
        {
                if (Node in Neighbor Table)
                {
                        if(RREQ Seen From different nexttolastAddress)→Process RREQ
                        else →Discard RREQ
                }
                else →Discard RREQ
        }

}
else →Insert into SeenRREQ Table
```

Figure 2.3 Node Spatiality Algorithm (Almobaideen et al, 2008).

In MSDMP, the destination or any intermediate node that has a valid route to the destination is responsible of selecting and recording the multiple node-disjoint paths. Any node generates a RREP for a specific RREQ must keep the list of the nodes participating in the path in the Replied RREQ Table. When a node receives a duplicate copy of a RREQ it must check its Replied RREQ Table to compare the Route List received in the RREQ with all stored entry for this RREQ. If there is not a common node (except source and destination) between the Route List of the current received RREQ and any route path recorded in the Replied RREQ Table. This means that the route path of the incoming RREQ satisfies the requirement of node-disjointness and is recorded in the Replied RREQ Table of the destination. Otherwise, the received RREQ is discarded (Almobaideen et al, 2008).

The filtering technique of the RREQ messages used in MSDMP reduces the overhead of processing RREQ packet, which was processed by neighbors, and this guarantees that the RREQ packets reach the destination will be spatially separated. This in turn will reduce the control overhead of discovering a route to the destination by discarding the RREQs that have been processed by neighbors (Almobaideen et al, 2008).

The idea behind choosing the spatially separated path is that allowing data to be sent on the most separated path insures that data transmission on one path will not be affected by the transmission on the others path which reduces the probability of collision that could occur. This in turn increases the network throughput and reduces the end-to-end delay (Almobaideen et al, 2008).

2.2 Multipath Routing Protocols for MANET's

In this section, we present some related research in multipath routing in ad hoc networks.

Li and Cuthbert proposed an extension of AODV called Node-Disjoint Multipath Routing protocol (NDMR). NDMR modifies AODV to allow path accumulation feature existed in DSR during route request packet transmission as well as discovering multiple node disjoint path. Simulation results showed that NDMR reduces routing overhead and achieved multiple node-disjoint multipaths (Li and Cuthbert, 2004).

In (Kim et al, 2006) Reverse-AODV (R-AODV) is proposed. R-AODV is a multipath searching method in which destination node uses reverse Route Request (RREQ) to find source node rather than a unicast reply. This technique reduces path fail correction messages and also source node builds partial or complete non-disjoint multipath from source to destination. In R-AODV, source node builds multipath to destination and adaptively hops available paths for data communications. Choosing paths based on hopping from one path to another can protect data from the intrusion of malicious nodes. The simulation results show the performance improvement gained by R-AODV over AODV in most metrics as end-to-end delay, packet delivery ratio and energy consumption.

A multipath extension to DSR is proposed In (Zafar et al, 2007) to support real time and multimedia applications. The proposed protocol called Shortest Multipath Source Routing (SMS). SMS builds multiple partial-disjoint paths from source to destination to reduce route discovery and to expedite recovery when a route is broken. Simulation results show that SMS reduces the end-to-end delay and the routing overheads as well as increasing the goodput when recovering from rout breakage.

Lee and Gerla proposed an On-demand routing protocol called Split Multipath Routing (SMR) in (Lee and Gerla, 2001). SMR is similar to DSR and uses a modified route request to find the maximally disjoint paths. The scheme proposed in SMR uses two routes for each session; the first is the shortest delay route and the second is the route, which is maximally disjoint with the shortest delay route. The discovered routes are used to send the data traffic to avoid the congestion on the network and to help in distributing the load over the network, which lead to efficient use of the network resources. The results show that SMR has fewer packet drops and end-to-end delay compared with DSR.

In (Meghanathan, 2007), Meghanathan presents a simulation-based analysis of the stability and hop count of node-disjoint and link-disjoint multi-path routes in mobile ad hoc networks. The results of the analysis showed that for different network density and node mobility, the node-disjoint paths were as stable as link-disjoint paths and these paths have not much difference in the hop count.

Grid-based Energy Aware Node-Disjoint Multipath Routing Algorithm (GEANDMRA) is proposed in (Wu et al, 2007). GEANDMRA uses concept of GRID routing protocols to propose an on-demand GRID-based routing algorithm. GEANDMRA differs from the GRID routing by considering the energy-aware and node-disjoint set of multipath. Simulation results indicate that GEANDMRA has much higher packet delivery ratio than the single path on-demand routing protocol such as AODV and DSR, as well as, less amount of end-to-end delay and routing load. The reason is that GEANDMRA discover energy-aware node disjoint path in contrast with AODV and DSR, which are single path routing, protocols.

In (Ge et al, 2008) authors use a location-based multiple zoning method to propose (M-Zon) protocol. Multiple Zones-based routing protocol discovers multiple node-disjoint paths segment by segment in large scale MANET's. Short delay and good scalability are the advantages of proactive and location based routing that M-Zon combines to discover node-disjoint paths effectively. M-Zon divides the region between the source and the destination into multiple zones to discover node-disjoint multiple paths using segment-by-segment route discovery. M-Zon uses two route maintenance approaches to maintain the routes; local and global route maintenance. The results show that M-Zon increase the average packet delivery ratio compared with a hybrid protocol that combines the ZRP protocol and the Global Positioning System (GPS) called GZRP.

A node disjoint multipath routing protocol for traffic load balancing is proposed in (Wu and Harms, 2001). The authors defined criteria for selecting the set of multipath. The correlation factor is a new metric defined between two node-disjoint paths as the number of the link connecting the two paths. In addition to the correlation factor, the selection criteria of path include the node-disjoint property as the first standard and the length difference between the primary path and the alternative paths. The routing algorithm proposed chooses the set of multiple paths that are node disjoint, have small difference between primary path and alternative paths and also have the minimum correlation factor, which in turn minimize the interference between transmissions in the individual paths.

In (Wu et al, 2007), a new routing algorithm called Ant-based Energy Aware Disjoint Multipath Routing Algorithm (AEADMRA) is proposed. AEADMRA is based on Ant colony algorithms, which are subset of swarm intelligence. Ant colony algorithms consider the ability of simple ants to solve complex problems by cooperation. AEADMRA develop the concept of GRID routing protocols to enable path accumulation in route request/reply packets and discover multiple energy aware routing paths with a low routing overhead. Simulation results indicate that AEADMRA outperforms GRID due to the discovering of energy aware disjoint routing paths that provide robustness to mobility.

2.3 Secure Routing Protocols for MANET's

Since security is an essential issue in ad hoc networks, many secure routing protocols have been proposed to mention the security challenges and issues related to routing in ad hoc network. Some of these protocols are discussed in this section.

Most of multipath routing protocols that consider spatiality focus on security issue. As in (Mavropodi et al, 2007) a complete secure multipath routing protocol is proposed. SecMR offers authentication in end-to-end and in link-to-link levels, and handles the integrity of the routing paths. SecMR works in two phases. The neighbouring authentication phase that is repeated in periodic time intervals and ensures the link-to-link authentication. While in the second phase, the signed request is generated by the source. This request gives the system an end-to-end authentication. Each intermediate node processes all the received requests to ensure that all possible node-disjoint paths will be finally discovered by the destination. The use of SecMR is dependent on the existence of Certificate Authority (CA), which led to problem during the period of CA unavailability.

In (Han et al, 2006), Multi-Path Security Aware Routing (MP-SAR) is suggested as improvement of the existed Security Aware Routing (SAR) protocol. MP-SAR keeps data confidentially offered by SAR and increases performance of data transmission speed. MP-SAR is a multiple secure path discovery algorithm that is based on AOMDV and transfers data quickly and reliably by using the shortest efficient path among the discovered multi-paths.

Bouam and Ben-Othman exploit the existence of multiple paths between nodes in an ad hoc network to introduce a solution for securing data transmission. The new solution which focuses on data security transmitting aspects is called Secured Data based Multipath routing protocol (SDMP). SDMP add a new layer placed on top of the transport (TCP/UDP) layer to manage the use of the proposed solution to secure sent data. In addition, a specific header, called SDMP header are added to get information to ensure security. SDMP divides the sent data messages and use existed multipath between source and destination. In this way, SDMP uses the advantage of the fact that even if an attacker succeeds to have one or lots of transmitted parts, the probability of original message reconstruction is low (BOUAM and BEN-OTHMAN, 2003).

In (Berton et al, 2006), Secure Disjoint Multipath Source Routing Protocol (SDMSR) for Mobile Ad-Hoc Networks proposed based on DSR. SDMSR solves the problem of secure routing in fully distributed MANET's using multipath routing with trade-off between maximally disjoint paths and message overhead. They combine two simple heuristics to get this trade-off. Firstly, it modifies the route discovery algorithm in that each node forwards a request if it is the first one or if the path of the incoming request is shorter than the precedent one. Secondly, it uses the MAC sub-layer neighbor's acknowledgement. When receiving a request, a node first probes its MAC layer to see if the destination is in its neighbourhood. If this is the case, the nodes unicast the request to the destination, and this will reduce the overhead caused by the first heuristic.

The Secure Efficient Ad hoc Distance vector (SEAD) is proposed in (Hu et al, 2002). SEAD is a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector (DSDV) algorithm. The SEAD routing protocol employs the use of hash chains to authenticate hop counts and sequence numbers. SEAD requires the existence of an authentication and key distribution scheme in order to authenticate one element of a hash chain between two nodes. Given this authenticated element, a node is able to verify later elements in the chain. The SEAD routing protocol proposes two different methods in order to authenticate the source of each routing update. The first method requires clock synchronization between the nodes that participate in the ad hoc network, and employs broadcast authentication mechanisms such. The second method requires the existence of a shared secret between each pair of nodes. This secret can be utilized in order to use a message authentication code (MAC) between the nodes that must authenticate a routing update message.

In (Talipov et al, 2006), the authors propose a path hopping method based on R-AODV (Kim et al, 2006). Path Hopping Reverse AODV (PHR-AODV) provides an analytic method to expect intrusion rate. In addition, the authors present a path hopping routing mechanism to build complete or partial node-disjoint multipath depending on the network topology. The performance evaluation of PHR-AODV compared with R-AODV and AODV is modelled using NS-2 simulation. Results show that PHR-AODV outperforms R-AODV and AODV in term of packet delivery ratio, energy consumption, and energy distribution as well as increasing security level of the network.

In (Zapata and Asokan, 2002), Secure Ad hoc On-demand Distance Vector (SAODV) is a proposal for security extensions to the AODV protocol. The proposed extensions use digital signatures and hash chains in order to secure AODV packets. Cryptographic signatures are used for authenticating the non-mutable fields of the messages, while a new one-way hash chain is created for every route discovery process to secure the hop-count field, which is the only mutable field of an AODV message. In SAODV, every route discovery that is initiated by a node corresponds to a new one-way hash chain. The elements of the chain are used in order to secure the metric field in the route request packets.

In (Virendra et al, 2007), the authors propose a network environment- aware trust-based route selection framework for Multi-Hop Wireless Networks (MWNs). The proposed framework uses a trust metric to adjust the route selection decisions. A node computes trust values for its neighbouring nodes and for the routes that pass through it. The trust metrics adaptively changes according to different network conditions and quick convergence of the protocol means it works well in different mobility scenarios. The results of (Virendra et al, 2007) were conducted using GloMoSim simulator and showed throughput improvement over conventional multipath protocols under congestion, link failure and route unreliability scenarios.

Ariadne is a secure on-demand ad hoc routing protocol based on DSR and provides end-to-end security mechanisms code in order to authenticate routing table entries for ad hoc networks. Ariadne employs a broadcast authentication protocol to authenticate broadcast messages, such as route requests. The most important requirement of Ariadne is the existence of clock synchronization in the ad hoc network.

The simulation results show that Ariadne is less efficient than the highly optimized version of DSR that runs in a trusted environment, since they did not secure the optimizations of DSR. The comparison between Ariadne with a version of DSR, in which they disabled all protocol optimizations not present in Ariadne shows that Ariadne actually performs better on some metrics than un-optimized DSR. The basic Ariadne protocol can be disrupted by wormhole attacks (Hu et al, 2002).

SECURE-PARTIALLY SPATIAL DISJOINT MULTIPATH ROUTING

3. Secure-Partially Spatial Disjoint Multipath Routing (S-PSDMP)

S-PSDMP is proposed as modification to the MSDMP (Almobaideen et al, 2008). S-PSDMP chooses the most spatially disjoint paths, which could join partially via nodes that specify certain security threshold. Using S-PSDMP, choosing partially disjoint paths that are most secure, could be better than choosing other maximally spatially disjoint paths that are less secure.

S-PSDMP modifies the RREQ message used in MSDMP by including the trust level of the node participated in the route path. Figure 3.3 shows the new RREQ message used in S-PSDMP. The Trust-Level List carries the trust value of each node participated in the Route-List.

Type	Flags	Hop Count
Last Address		
Next to Last Address		
Broadcast ID		
Destination Address		
Destination Sequence Number		
Originator Address		
Originator Sequence Number		
Route List		
Trust Level List		

Figure 3.1: S-PSDMP RREQ Message Format.

As in MSDMP, when an intermediate node decides to rebroadcast a RREQ packet it must add its own address on the Route List. In S-PSDMP the trust value must be added to the Trust-Level List in the RREQ packet. Any node checks the disjointness of the path and before generating a RREP packet on a specific path it must check the Trust level of all the nodes participating in the path. If the path has a node with trust value less than a certain trust threshold this path will not be used and the RREQ will be discarded. We call the protocol that uses this method as Secure Maximally Disjoint Multipath Routing Protocol (S-MSDMP). S-MSDMP will be used later in this thesis to be compared with S-PSDMP.

In S-PSDMP we modify the maximally node disjoint algorithm built in MSDMP by allowing the path to be partially disjoint via nodes that specify certain trust threshold. When an intermediate node checks the disjointness of a certain path and there is a common node in this path, a check of trust level of this common node is made. If the trust level of the common node exceeds a certain threshold value, this path will be considered in the selection process of multipath.

In S-PSDMP, choosing secure partially spatial disjoints path acquire the improvement obtained by MSDMP while taking security measures in concern. MSDMP sends data using spatially separated path and it is proven that sending data packets in this way increases the network performance by minimizing the probability of collision between nodes sending data on different paths (Almobaideen et al, 2008). S-MSDMP transmits data on a less number of paths than MSDMP but S-MSDMP assures that the transmitted data passed through secure nodes.

RESULTS AND ANALYSIS

4. Results and Analysis

4.1 Introduction

In this chapter, we will give an overview about the simulator used in our experiments, followed by the simulation results and their analysis. In this thesis the Global Mobile Information System Simulation Library network simulator (GloMoSim) was used to evaluate the performance of the S-PSDMP. Different performance metrics were used to compare S-PSDMP with the S-MSDMP and it will be described in section.

4.2 What is GloMoSim?

GloMoSim is a library that can be used when simulating wireless networks. It is designed to support scalable simulation environment for wireless and wire-line communication networks. GloMoSim uses a parallel execution to reduce the simulation time implemented in GloMoSim simulator (Nuevo, 2004) and (Zeng et al, 1998)

The design of the GloMoSim simulator is based on a set of library modules, each one of these module implements different functionalities of different wireless communication protocols of the protocol stack. Table 4.1 lists the protocols implemented in GloMoSim with the available modules at each layer (Nuevo, 2004)

Table 4.1 GloMoSim Layers (Nuevo, 2004),

Layer	Models
Physical (Radio Propagation)	Free space, Two-Ray
Data Link (MAC)	CSMA,MACA,TSMA,802.11
Network (Routing)	Bellman-Ford,FSR,OSPF, DSR, WRP, LAR, AODV
Transport	TCP, UDP
Application	Telnet, FTP

4.3 Simulation Environment

In the experiments we have conducted in this thesis the simulation modeled a network of 100 mobile hosts placed randomly within a 2000X2000 meters area. We used Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. In the experimental scenarios, the mobile nodes have been moving randomly for 400 seconds simulation time. Each node moves independently according to the random waypoint mobility model with a 25 (Meter/Second) as maximum mobility speed and 25 S as pause time. The simulated traffic is a Constant Bit Rate (CBR).The size of application data was 512 bytes.

Each experiment has been repeated at least 25 times using different seeds and an average value of these runs has been computed to represent the final resulted value of the measured performance metric.

4.4 Performance Metrics

We use the following performance metrics to compare the performance of S-PSDMP and S-MSDMP protocols:

- Network Throughput: Throughput is calculated as received throughput in Kb/sec received at the traffic destination.
- Average end-to-end Delay: The end-to-end delay is averaged for all data packet delivered successfully from the sources to the destinations.
- Routing Overhead: The routing overhead is measured as the average number of control packets transmitted at each node during the simulation.
- Participation Ratio: The participation ratio is computed as the average number of data packet received at intermediate nodes involved in a path between a source-destination pairs.

4.5 Improvement Ratio

To show the enhancement obtained by S-PSDMP regarding the selected performance metrics and parameters we present the improvement ratio to help in the comparison between S-PSDMP and S-MSDMP. Improvement Ratio (IR) of both protocols can be computed according to Formula 1.

IR= (P- M) / P …....................................…... Formula 1

Where P: value of S-PSDMP

M: value of S-MSDMP.

4.6 Results and Analysis

In this section, we present the results and their analysis of the proposed S-PSDMP protocol regarding the mentioned performance parameters and metrics. We compare the results of the proposed S-PSDMP with S-MSDMP. In order to compare a protocol that has security concern such as MSDMP with an S-PSDMP that has not, we introduce S-MSDMP that uses the same techniques in MSDMP but chooses the set of paths that satisfy the security level in addition to being concerned with maximally spatially disjoint paths.

4.6.1 Different Traffic Load

In order to change the traffic load of the network we increase the number of packets the traffic source has to send ranging from 20,40,60,80 to 100 packets. Figure 4.1 compares between the average end-to-end delay of S-PSDMP and S-MSDMP while changing the traffic load. The improvement of S-PSDMP is clear, especially as the traffic increases.

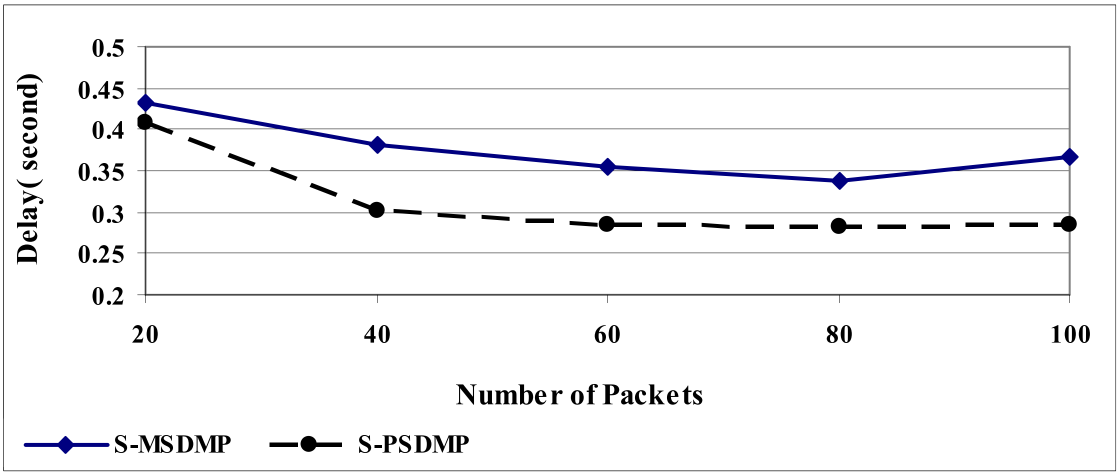


Figure 4.1: Average End-to-End delay Vs. Number of Packets.

The reduction of delay gained by S-PSDMP is because S-PSDMP chooses the set of multipath with less number of constraints than in S-MSDMP, since S-PSDMP chooses the paths that could join partially via a trusted node in contrast with S-MSDMP which chooses only the maximally disjoint paths. The result of this is that while using S-PSDMP a traffic source gets larger number of paths than when using S-MSDMP. This in turn reduces the delay needed by the source to discover a new path if the existing path becomes invalid or broken. According to this experiment, the improvement ratio of delay reduction gained by S-PSDMP is 21%.

In Figure 4.2, we show the discovery overhead of the two protocols as the traffic load increases. Although S-PSDMP employs the same filtering techniques used in S-MSDMP, but its clear that S-PSDMP has lower discovery overhead than S-MSDMP and this is because by using S-PSDMP there is a greater number of discovered path than with S-MSDMP. The discovered set of paths will be used when the existing one becomes broken. The improvement ratio of discovery overhead reduction gained by S-PSDMP in this experiment is 5%.

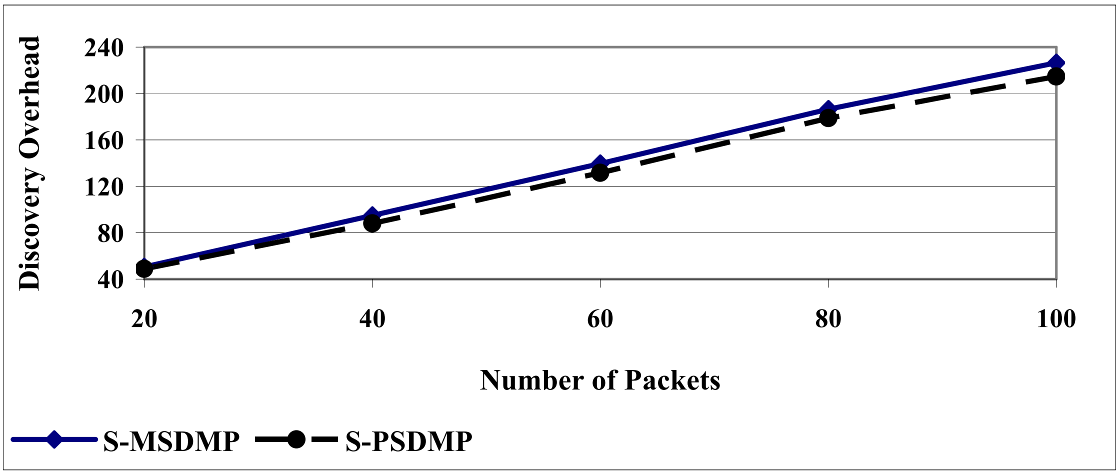


Figure 4.2: Discovery Overhead Vs. Number of Packets.

Figure 4.3 presents the comparison of throughput for the two protocols. It is clear that S-PSDMP outperforms S-MSDMP especially when the traffic load is small. The improvement ratio of throughput gained by S-PSDMP is 2%. The throughput of both S-PSDMP and S-MSDMP decreases as the traffic load increases and this happen due to the fact that when the traffic load increases, nodes in the network will be overloaded which oblige them to drop packets. Congestion on the network introduces more delay and as a result, it will decrease the throughput. Although S-PSDMP has security constraints that govern the selection of the multipath, it still has a greater throughput than S-MSDMP.

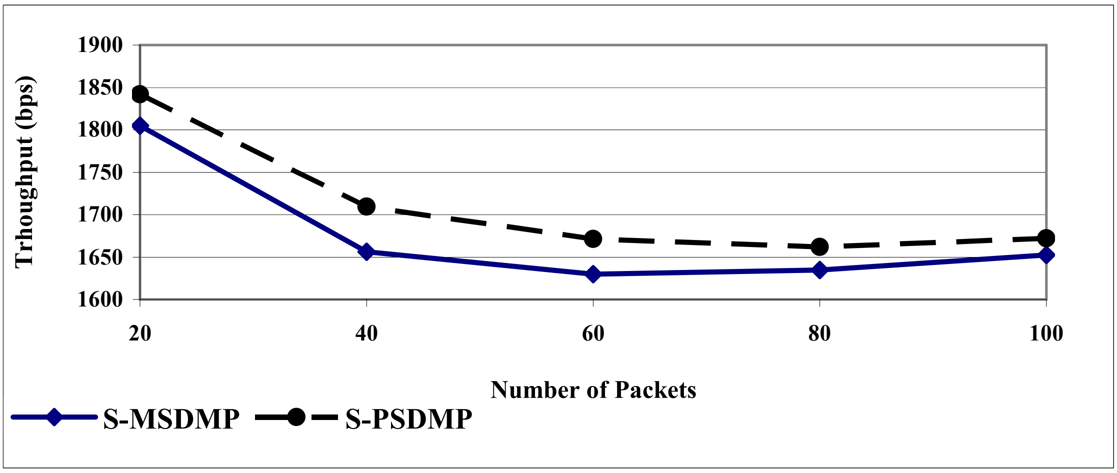


Figure 4.3: Throughput vs. Number of Packets.

4.6.2 Varying Node Density

In the next three experiments, nodes density is considered as the performance parameter in the evaluation of the two protocols regarding same performance metrics mentioned above. In order to change the density of nodes in the simulated terrain a gradual increment of the terrain area was done in order to move to a sparser mode. The successive experimental scenarios assume a terrain with a side length ranging from 500, 1000, 1500, 2000, 2500, and up to 3000 meters.

An experiment is conducted to compare the end-to-end delay of S-PSDMP and S-MSDMP while changing the nodes density expressed by using the length of the terrain side. The result of this experiment is shown in Figure 4.4. The figure illustrates that as the density of nodes decreases, S-PSDMP incurs less delay compared with S-MSDMP. This is because, in contrast with S-MSDMP, S-PSDMP chooses partially disjoint paths based on trust level of the nodes. Choosing partially disjoint paths increases the number of selected multipath and as a result decreases the delay resulting from the extra time needed to discover a new path when the existed path becomes broken or invalid. The improvement ratio of delay reduction gained by S-PSDMP in this experiment is 13%.

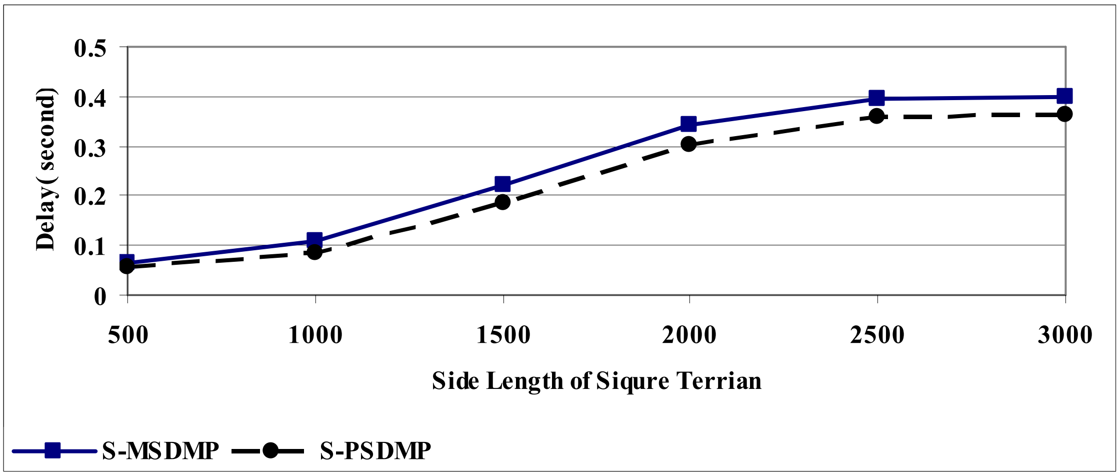


Figure 4.4: Average End-to-End Delay vs. Terrain Dimension.

Figure 4.5 shows a comparison of discovery overhead between S-PSDMP and S-MSDMP. The discovery overhead of both S-PSDMP and S-MSDMP increases as the density of nodes decreases and this happens because when nodes become sparser the probability of path breakage becomes higher due to the node mobility. Frequent path breakage will invoke the route discovery mechanism which introduces overhead in the network. We can obtain form the figure that S-PSDMP has smaller discovery overhead than that of S-MSDMP since S-PSDMP has a greater number of selected paths which makes the invocation of the route discovery mechanism happen less than S-MSDMP in the case of route breakage. The improvement ratio of discovery overhead reduction gained by S-PSDMP in this experiment is 5%.

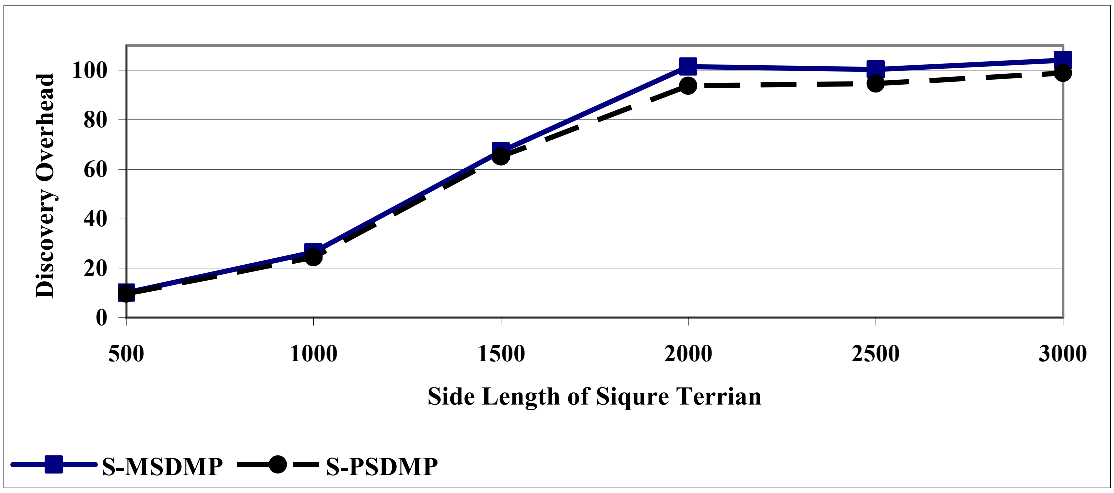


Figure 4.5: Discovery Overhead Vs. Terrain Dimension

In Figure 4.6, we present a comparison of throughput between S-PSDMP and S-MSDMP as the density of node decreases. We can notice from the figure that S-PSDMP gains higher throughput than S-MSDMP as the nodes become sparser with improvement ratio of 1.5%. In addition, the figure shows that throughput of both protocols is decreases as the nodes become sparser and this happens because when the nodes become sparser, path breakage probability becomes greater which introduces more discovery overhead and delay and as a result decreases the throughput.

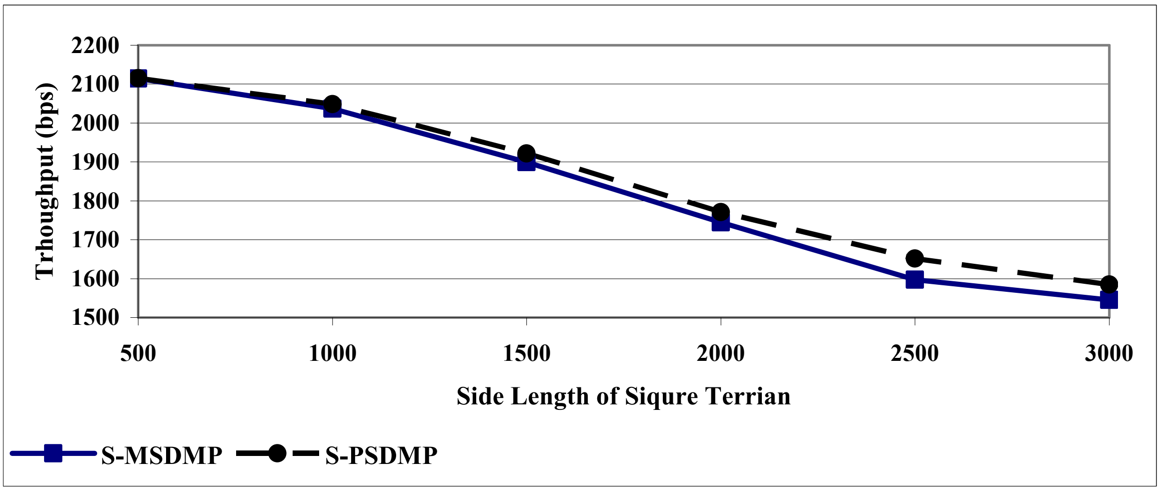


Figure 4.6: Throughput vs. Terrain Dimension

To compare the participation ratio of nodes in both S-PSDMP and S-MSDMP, an experiment has been conducted; see Figure 4.7, in which the node density has been varied in same way of pervious experiments. The figure shows that the S-PSDMP has greater amount of participation ratio than S-MSDMP and this due to the fact that with S-PSDMP the selected path is partially node-disjoint which means a node could participate in more than one path between source-destination pair. In this case, the number of data packet received by this node will be greater than the previous one while using S-MSDMP.

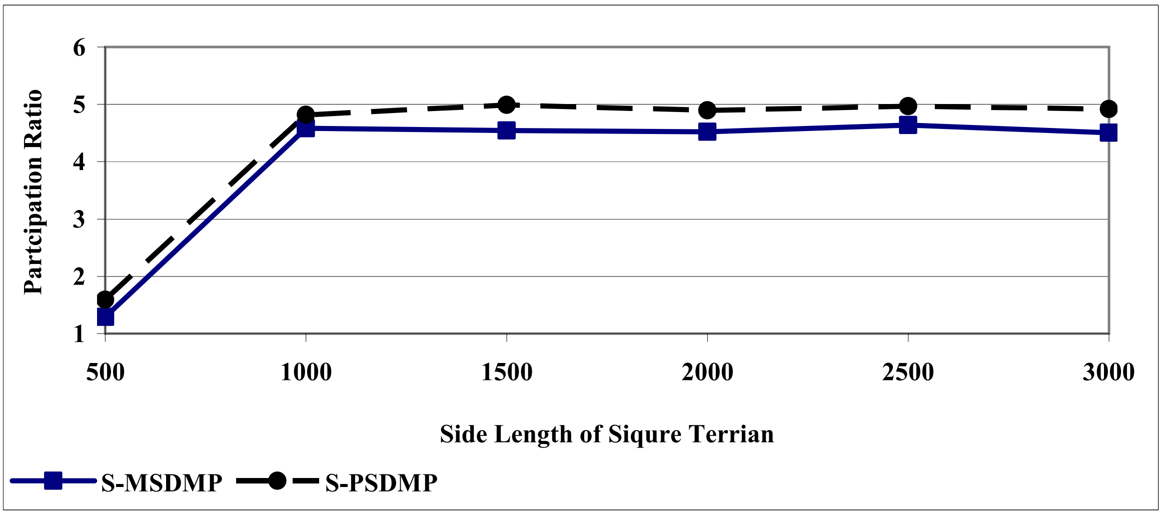


Figure 4.7: Participation Ratio vs. Terrain Dimension

4.6.3 Different Number of Maximum Allowed Path

In the next set of experiments, we increase the maximum allowed number of multiple path that can be stored at a source to a specific destination. We started from two paths since we are interested in multipath routing. The number of paths increased to six paths.

The result of the first experiment is presented in figure 4.8. We can notice from the figure that S-PSDMP incurs less end-to-end delay than S-MSDMP with improvement ratio of 6%. This is because in contrast with S-MSDMP, S-PSDMP chooses not only the maximally spatially disjoint multipath, but also the paths that could join partially at trusted node. Choosing multipath based on these criteria increases the number of selected paths which could be used to send data packet. Sending packets over greater number of path reduces the average end-to-end delay in case of path breakage.

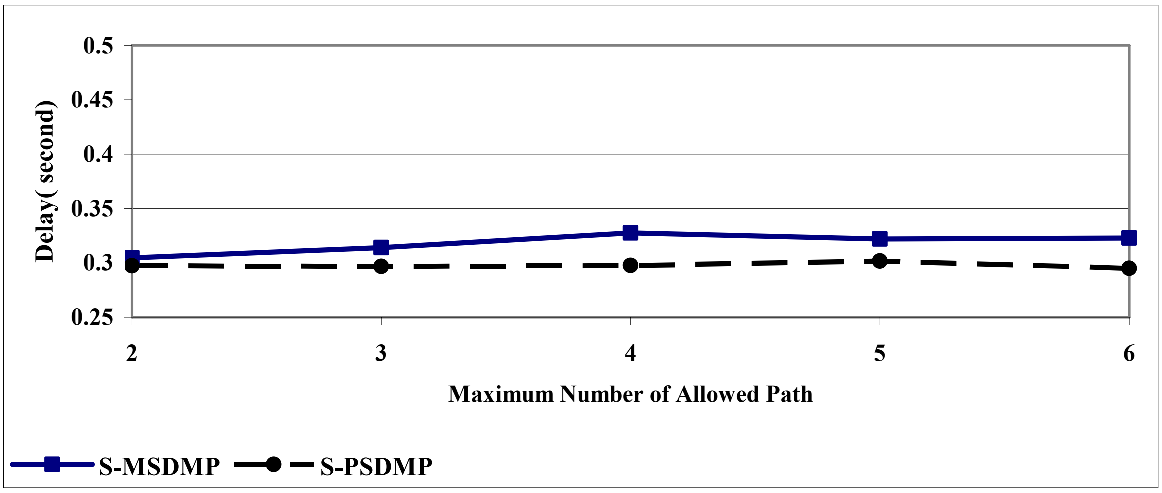


Figure 4.8: Average End-to-End Delay vs. Maximum Number of Allowed Path

Figure 4.9 shows comparison between S-PSDMP and S-MSDMP routing protocols in term of discovery overhead when the maximum allowed number of path increases. The figure illustrates that S-PSDMP encounters much less overhead than S-MSDMP since S-PSDMP chooses a greater number of alternative paths that could be used without invocation of the route discovery process in case of path breakage or invalidation. The improvement ratio of discovery overhead reduction in this experiment is 6%.

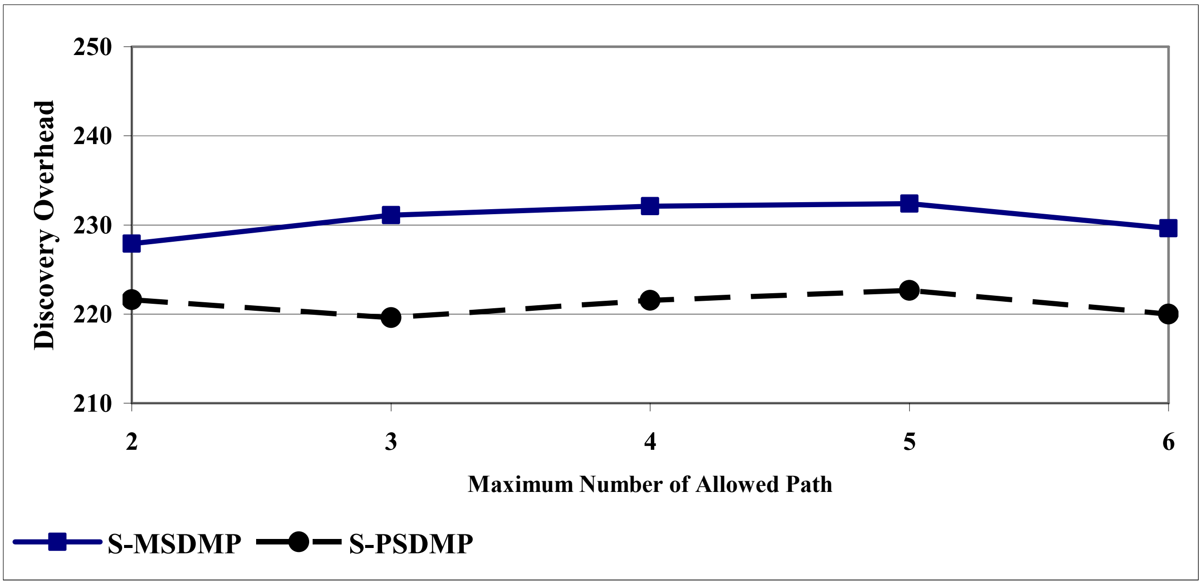


Figure 4.9: Discovery Overhead Vs. Maximum Number of Allowed Path

The effect of increasing the maximum number of allowed path on the throughput is shown in Figure 4.10. One can notice from the figure that S-PSDMP gives the greatest throughput difference with maximum number of allowed path equals three. It is clear that S-PSDMP obtains higher throughput than S-MDMP as the number of maximally allowed path increased with improvement ratio of 2%. S-PSDMP chooses a greater number of paths to send data packet which reduces the delay and as a result increases the throughput.

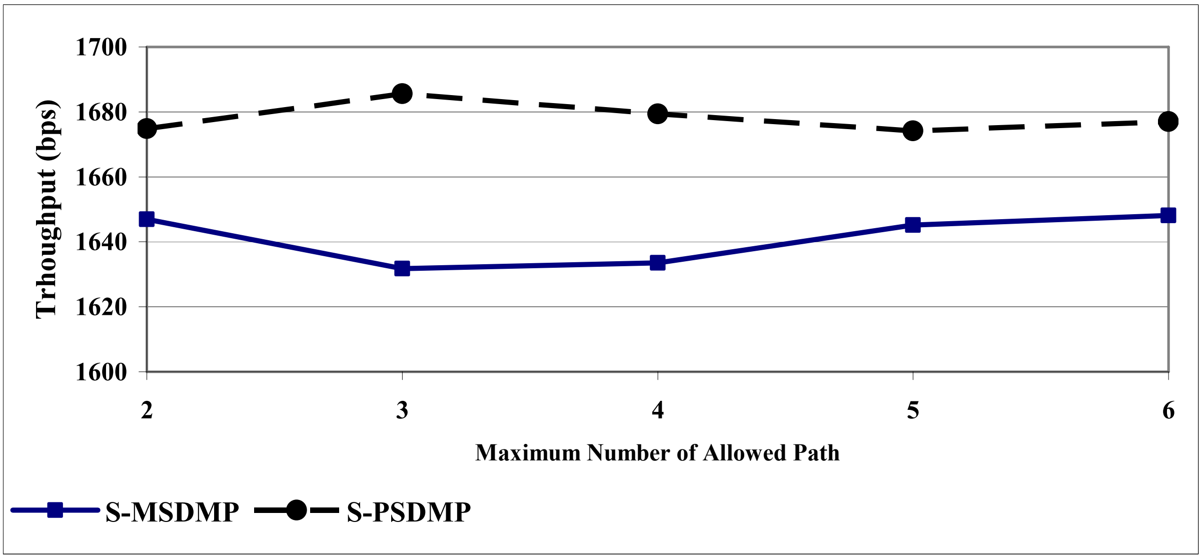


Figure 4.10: Throughput vs. Maximum Number of Allowed Path

Figure 4.11 presents a comparison of participation ratio between S-PSDMP and S-PSMP as the number of maximum allowed number increases. We can notice that the S-PSDMP has great amount of participation ratio than S-MSDMP and this happens due to the fact that S-PSDMP chooses set of paths which could join partially via nodes satisfy certain trust level, this means a node could participate in more than one path between source- destination pair, which in turn increases the number of data packet received at nodes.

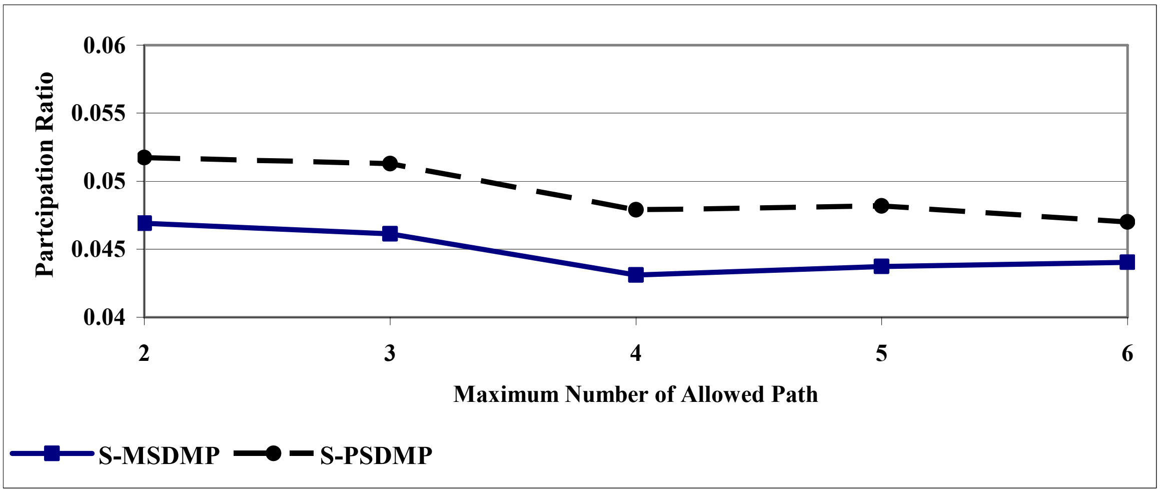


Figure 4.11: Participation Ratio vs. Maximum Number of Allowed Path

5. CONCLUSIONS AND FUTURE WORKS

5. Conclusions and Future Work

5.1 Conclusions

In this thesis we have proposed the S-PSDMP routing protocol as a security enhancement to the MSDMP. S-PSDMP chooses the most spatially disjoint paths which could join partially via nodes that specify certain security threshold. S-PSDMP exploits a trusted node to participate in the selected set of route between a source and destination

Different performance metrics were used to compare S-PSDMP and S-MSDMP includes the average end-to-end delay, throughput, discovery overhead, participation ratio, and packet delivery ratio. Traffic load, nodes density, and the maximum number of allowed path are chosen as performance parameters to S-PSDMP and S-MSDMP to the previous performance.

The simulation results have showed that the S-PSDMP obtain higher throughput than S-MSDMP under different networks conditions. In addition S-PSDMP incurs less average end-to-end delay and discovery overhead than that of S-MSDMP.

Although the results have showed that S-PSDMP has great amount of participation ratio than S-MSDMP, still the participated nodes in a path is trusted which means that the sent packet will be protected during transmission when using S-PSDMP in contrast with S-MSDMP.

To help in comparison between S-PSDMP and S-MSDMP we present the Improvement Ratio obtained by S-PSDMP regarding to the selected performance metrics and parameters. Table 2 shows the throughput improvement ratio gained by S-PSDMP.

Table 2 Throughput Improvement Ratio

Performance Parameter	IR
Varying Traffic Load	0.0221
Varying Node Density	0.0151
Varying Number of Path	0.0221

Table 3 shows the Improvement Ratio of reducing the discovery overhead by S-PSDMP. It is clear that S-PSDMP incurs less overhead than that of S-MSDMP in all experiments.

Table 3 Discovery Overhead Improvement Ratio

Performance Parameter	IR
Varying Traffic Load	-0.05339
Varying Node Density	-0.05479
Varying Number of Path	-0.04138

In Table 4 we present the Improvement Ratio of reducing the average end-to-end delay achieved by S-PSDMP. One can notice that S-PSDMP incurs less average end-to-end delay with all performance parameters.

Table 4 Delay Improvement Ratio

Performance Parameter	IR
Varying Traffic Load	-0.21271
Varying Node Density	-0.13517
Varying Number of Path	-0.06418

5.2 Future Work:

In our study we choose the set of spatial disjoint paths which could join partially via nodes that specify certain trust threshold. The trust value is randomly assigned to the nodes in the network. As future work, we propose to compute the trust level of each node based on the properties of the set of discovered multipath and statistical information about how each of these paths behaves on the network.

To show the security improvements gained by the propped S-PSDMP, we need to analyze the results according to security measurement as future work.

REFERENCES

References

Abolhasan, M., Wysocki, T., and Dutikiewwicz, E., (2004), A review of routing protocols for mobile ad hoc networks, **Ad Hoc Networks 1,(**2) , pp.:1-22.

Almobaideen, W., Sleit, A., Qatawneh, M., and Al-Soub, R. (2008), MSDMP: Maximally Spatial Disjoint Multipath Routing Protocol over MANETs, **submitted to computer communications.**

Argyroudis, P. G. and O'Mahony, D.(2004), Secure Routing for Mobile Ad hoc Networks, **Communications Surveys & Tutorials,** IEEE 2005, 7(3), pp.2- 21.

Berton, S., Yin, H., Lin, C. and Min, G. (2006) Secure, Disjoint, Multipath Source Routing Protocol(SDMSR) for Mobile Ad-Hoc Networks, **Proceedings of the Fifth International Conference on Grid and Cooperative Computing** (GCC'06), IEEE Computer Society, Washington, DC, USA 2006**.** pp. 387 – 394,

BOUAM, S., BEN-OTHMAN, J. (2003), Data Security in Ad hoc Networks Using MultiPath Routing, **Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003.** (2), pp. 1331–1335.

Chakeres, I. D., Belding-Royer E. M. (2004), AODV Routing Protocol Implementation Design**, In the Proceedings of the 4th International Conference of the Distributed Computing Systems Workshops,** 2004. pp. 698- 703.

Crow, B. P., Widjaja, I., Kim, J. G., Sakai, P.T. (1997), IEEE 802.11 Wireless Local Area Networks, **IEEE Communications Magazine**. (1997), 0163-6804.

Ge, Y., Wang, G., Jia, W. and Xie, Y. (2008), Node-Disjoint Multipath Routing with Zoning Method in MANET's, **High Performance Computing and Communications, 2008. HPCC '08.** pp. 456-462.

Han, I. S., Ryou, H. B. and Kang S. J. (2006), Multi-Path Security-Aware Routing Protocol Mechanism for Ad Hoc Network, **International Conference on Hybrid Information Technology (ICHIT'O6)**, IEEE Computer Society. pp. 620-626,

Heide Clausen, T., Jacquet, P., and Viennot, L. (2002) Comparative Study of Routing Protocols for Mobile Ad-hoc NETworks, **In Proceeding of The First Annual Mediterranean Ad Hoc Networking Workshop 2002.** MindPass Center for Distributed Systems, Aalborg University and Project Hipercom, INRIA Rocquencourt.

Hu, Y. C., Johnson, D.B. and Perrig, A. (2003), SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks**, Ad Hoc Network**s, (1)1, July 2003, pp. 175-192.

Hu, Y. C., Perrig, A., and Johnson, D.B. (2002), Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks, **Proc. 8th ACM Int'l. Conference of Mobile Computing and Networking (Mobicom'02),** Atlanta, Georgia, September 2002, pp. 12-23.

IEEE 802 LAN/MAN STANDARDS COMMITTEE. IEEE 802.11 (2007), Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, (Revision of IEEE Std 802.11-1999).

Johnson, D. B., Maltz, D. A. (1996), Dynamic source routing in ad hoc wireless networks, **Mobile Computing**, edited by Tomasz Imielinski and Hank Korth, Chapter 5, Kluwer Academic Publishers, 1996, pp. 153-181.

Kim, C., Talipov, E. and Ahn, B. (2006), A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks, in **Directions in Embedded and Ubiquitous Computing**, **LNCS**(4097), pp. 522 – 531, Springer Berlin-Heidelberg.

Lee, S. J. and Gerla, M. (2001), Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks, **In Proceedings of the IEEE International Conference IEEE ICC**, Volume: 10, pp. 3201-3205, 2001.

Li, X. and Cuthbert, L. (2004),On-demand Node-Disjoint Multipath Routing in Wireless Ad hoc Networks, **Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks** (LCN'04), pp. 419- 420

Liu, C., Kaiser, J. (2005), A Survey of Mobile Ad Hoc network Routing Protocols, **University of Ulm Tech.Report Series**, Nr. 2003-08.

Marina, M. K. and Das, S. R. (2001), On-demand Multipath Distance Vector Routing in Ad Hoc Networks, **in Proceedings of IEEE International conference on Network Protocols (ICNP)**, pp. 14-23.

Mavropodi, R., and Douligeris, C. (2006), Multipath Routing Protocols for Mobile Ad Hoc Networks: Security Issues and performance Evaluation**, in Autonomic Communication, LNCS** (3854), pp.165 -176, Springer Berlin- Heidelberg.

Mavropodi, R., Kotzanikolaou, P. and Douligeris, C. (2007), SecMR – a secure multipath routing protocol for ad hoc networks, **Ad Hoc Networks,** 5 (2007), pp. 87–99.

Meghanathan, N. (2007), Stability and Hop Count of Node-Disjoint and Link-Disjoint Multi-Path Routes in Ad Hoc Networks, **In Proceedings of the Third IEEE international Conference on Wireless and Mobile Computing, Networking and Communications** (October 08 - 10, 2007). WIMOB. IEEE Computer Society, Washington, DC, 42.

Nuevo, J. (2004), a Comprehensible GloMoSim Tutorial, Mltihops at **www.externe.inrs-emt.uquebec.ca/users/nuevo/glomoman.pdf,**

Perkins, C. E., and Royer, E. M. (1999), Ad hoc On-demand Distance Vector Routing, **proceedings of the 2nd Annual IEEE International Workshop on Mobile Computing Systems and Applications**, pp. 90 – 100, February 1999.

Royer, E., and Toh, C-K. (1999), A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, **IEEE Personal Communications**, 6(2), pp. 46-55.

Talipov, E., Jin, D., Jung, J., Ha, I., Choi, Y. and Kim, C. (2006), Path Hopping Based on Reverse AODV for Security, **in Management of Convergence Networks and Services,** LNCS (4238) , pp. 574 – 577, Springer Berlin- Heidelberg.

Virendra, M., Krishnamurthy, A., Narayanan, K., Upadhyaya, S. and Kwiat K. (2007), Environment-Aware Trusted Data Delivery in Multipath Wireless Protocols, in **Computer Network Security**, CCIS (1), pp.396 -401, Springer Berlin-Heidelberg.

Wu, K. and Harms, J. (2001), Performance study of a multipath routing method for wireless mobile ad hoc networks, **In Proceedings of the Ninth international Symposium in Modeling, Analysis and Simulation of Computer and Telecommunication Systems** (Mascots'01) (August 15 - 18, 2001).

Wu, Z., Dong, X. and Cui, L. (2007), A Grid-based Energy Aware Node-Disjoint Multipath Routing Algorithm for MANET's**, In Proceedings of the Third international Conference on Natural Computation** (ICNC 2007) - Volume 05 (August 24 - 27, 2007). ICNC.pp. 244-248.

Wu, Z., Song, H., Jiang, S. and Xu, X. (2007), Ant-based Energy Aware Disjoint Multipath Routing Algorithm in MANET's, **In Proceedings of the 2007 international**

Conference on Multimedia and Ubiquitous Engineering (April 26 - 28, 2007). MUE, pp.674-679.

Zafar, H., Harle, D., Andonovic, I. and Ashraf, M. (2007), Partial-Disjoint Multipath Routing for Wireless Ad-hoc Networks, **In Proceedings of the 32nd IEEE Conference on Local Computer Networks** (October 15 - 18, 2007), pp. 258-259.

Zapata, M.G. and Asokan, N. (2002), Secure Ad hoc On-Demand Distance Vector Routing, **ACM Mobile Computing and Communications Review**, (3) , 6, July 2002, pp. 106-107.

Zeng, X., Bagrodia, R., and Gerla, M., (1998), GloMoSim: a Library for Parallel Simulation of Large-Scale Wireless Networks, pads, **In Proceedings of 12th Workshop on Parallel and Distributed Simulation (PADS'98**), pp. 154.

Zhou, L. and Haas, Z. (1999), Securing Ad Hoc Networks, **IEEE Networks Special Issue on Network Security**. November/December 1999, pp. 24-30.

مسارات آمنه متصلة جزئياً منفصلة مكانياً لشبكات التنقل العشوائي

إعداد
ربا خالد محمد الصعوب

المشرف
الدكتور وسام عبد الرحمن المبيضين

المشرف المشارك
الدكتور عزام طلال سليط

ملخص

في السنوات القليلة الماضية أصبح هناك اهتمام متزايد في شبكات التنقل العشوائي(MANETs) وذلك لتعدد تطبيقاتها. من الصعب اختيار أفضل المسارات لاستخدامها في الإرسال في MANETs وقد تم اقتراح العديد من بروتوكولات التوجيه لإعطاء حلول للمشاكل التي برزت في هذا النوع من الشبكات. تعد بروتوكول التوجيه التفاعلي (عند الطلب) احد أنواع البروتوكولات المستخدمة في MANETs . يعد استخدام بروتوكولات التوجيه متعددة المسارات من أهم الاتجاهات البحثية المتعلقة في الإرسال على هذا النوع من الشبكات. البحوث الحديثة بدأت في التركيز على بروتوكولات التوجيه متعددة المسارات للحصول على فاعلية أفضل في الإرسال، القدرة على العمل بوجود الأخطاء، والتوازن في توزيع عبء الإرسال على المسارات باختلاف الظروف في الشبكة.

مع الاهتمام المتزايد في شبكات التنقل العشوائي، أصبح هناك تركيز كبير على قضايا الأمان في هذه الشبكات. يوجد العديد من الأبحاث تهدف إلى تصميم بروتوكولات مخصصة لاختيار مسارات آمنة في الشبكات وذلك من أجل توفير الحماية ضد نوع أو أكثر من الاختراقات. في هذه الرسالة نعرض بروتوكول يختار مسارات أمنه متصلة جزئياً منفصلة مكانياً لشبكات التنقل العشوائي ، يقوم على إضافة قضية الأمان لبرتوكول سابق يختار مسارات منفصلة مكانياً بشكل تام. البروتوكول المقترح يقوم على اختيار المسارات المتباعدة مكانياً والتي من الممكن أن تتصل جزئياً بواسطة أجهزة تحقق مستوى معين من الأمان.

اثبتت النتائج أن البروتوكول المقترح زاد أداء الشبكة وقلل من التأخير وعبء إيجاد الطريق عند مقارنته مع البروتوكول الذي يختار مسارات أمنه منفصلة مكانياً بشكل تام. كان معدل نسبة التحسين في أداء الشبكة 2% ، وكانت نسبة التحسين في تقليل التأخير وعبء إيجاد الطريق 14% و5% على التوالي.