ENHANCEMENT OF ADHOC ON-DEMAND DISTANCE VECTOR PROTOCOL SECURITY USING SECURE MESSAGE TRANSMISSION

A Thesis by

Satya Balagam

Bachelor of Engineering, Andhra University, 2007

Submitted to the Department of Electrical Engineering and Computer Science
and the faculty of Graduate School of
Wichita State University
in partial fulfillment of
the requirements for the degree of
Master of Science

December 2011

ENHANCEMENT OF AD HOC ON-DEMAND DISTANCE VECTOR PROTOCOL SECURITY USING SECURE MESSAGE TRANSMISSION

The following faculty members have examined the final copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirement for the degree of Master of Science with a major in Electrical Engineering.

_____
Neeraj Jaggi, Committee Chair

_____
Bin Tang, Committee Member

_____
Krishna Krishnan, Committee Member

ABSTRACT

The ad hoc on-demand distance vector (AODV) routing protocol offers quick adaptation to dynamic link changes, incurs low processing and memory overhead, has a low initial setup while connecting to networks, and determines unicast routes to destinations within the ad hoc network. This routing protocol allows for efficient and reliable discovery of routes. Although the connection setup delay is lower for the AODV protocol compared to other ad hoc routing protocols, such as the dynamic source routing (DSR) protocol and destination sequenced distance vector (DSDV) protocol, the AODV routing protocol involves a heavy control overload and delay while finding the routes in adverse conditions, such as the presence of malicious nodes in the network or connection failures due to network congestion.

This thesis studies the secure message transmission (SMT) protocol, which safeguards data transmission against arbitrary malicious behavior of other nodes and evaluates its performance over the AODV routing protocol. The analysis of the performance of the AODV routing protocol in combination with the SMT protocol was done by considering a scenario of mobile ad hoc networks under adverse conditions, with half of the nodes acting maliciously and dropping both data and control packets. The AODV routing protocol in combination with the SMT protocol imposes up to 46% less routing overhead, delivering up to 17% more data packets, with a throughput of 12% more and end-to-end delays that are up to 24% lower than those of the native AODV routing protocols in the scenarios considered. Thus the AODV routing protocol performs well with the SMT protocol, and is reliable. The NS-2 network simulator was utilized to compare performances. The advantages of the proposed approach of using the AODV routing protocol together with the SMT protocol are more apparent in the presence of malicious nodes in the network.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

TABLE OF CONTENTS (continued)

Chapter Page

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS/NOMENCLATURE

ABR	Associativity-Based Routing
AODV	Ad Hoc On-Demand Distance Vector
AODV-UU	Ad Hoc On-Demand Distance Vector – University of Uppsala
APS	Active Path Set
CBR	Constant Bit Rate
CBRP	Constant Bit Rate Period
CGSR	Cluster-Head Switch Routing
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
DV	Distance Vector
FIFO	First In First Out
FSR	Fisheye State Routing
HNA	Host and Network Association
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
MAC	Message Authentication Code
MACT	Multicast Activation
MANET	Mobile Ad hoc Networks
MPRs	Multi Point Relays

NAM	Network Animator
NIST	National Institute of Standards and Technology
NS	Network Simulator
NS-2	Network Simulator 2
PDR	Packet Delivery Ratio
PK	Public Key
PKA	Public Key Authentication
RDMAR	Relative Distance Micro-discovery Ad Hoc Routing
RREP	Route Replies
RREP-ACK	Route Reply Acknowledge
RREQ	Route Requests
RERR	Route Errors
SMT	Secure Message Transmission
TC	Topology Control
TCP	Transmission Control Protocol
TORA	Temporarily Ordered Routing Algorithm
TTL	Time to Live
UDP	User Datagram Protocol
VANET	Vehicular Ad Hoc Networks
V_{max}	Maximum Speed
V_{min}	Minimum Speed
VNIT	Visvesvaraya National Institute of Technology

WiFi	Wireless Fidelity
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network
WRP	Wireless Routing Protocol
ZRP	Zone Routing Protocol

CHAPTER 1

INTRODUCTION

1.1 Ad Hoc Networks

The word *ad hoc,* meaning "solely," is derived from Latin. The network is known as ad hoc because there is no dependence on a preexisting infrastructure such as routers or access points. The reliance of the network on a base station for the coordination of data flow among the nodes is eliminated by the communication between individual nodes. To achieve this, the nodes forward packets among themselves.

In the context of a wireless computer network, the ad hoc mode is a method of communication among the wireless devices without the need for infrastructure. The operation in ad hoc mode involves all wireless devices communicating with each other without having a central access point.

As shown in Figure 1.1, ad hoc networks do not involve access points to transfer data between nodes. Typically, infrastructure networks have a central hub through which the data transfers throughout the network. For example, in an office scenario, there is a server through which other work stations are connected. In contrast, ad hoc networks do not have a centralized hub but rather connect through their peers. These are generally intranets or networks that operate only between nodes. They can connect to the Internet if one of the participants has a connection to the Internet through a public or private network, and the connection can be shared among the nodes in the ad hoc network.

General uses of ad hoc networks include portable video game systems such as Microsoft Xbox or the Sony PSP. These systems allow players to connect to each other over a wireless link. Electronic stores are also developing various ideas like setting up their own ad hoc

networks to allow players to download games directly from their company. Thus, an ad hoc network acts as a peer-to-peer network sans wires as shown in Figure 1.2. Used in the development for early Windows computers, this type of system allows computers to connect to each other in a small environment where each node is available within the range, without the establishment of domains and thus eliminating overhead costs [1].

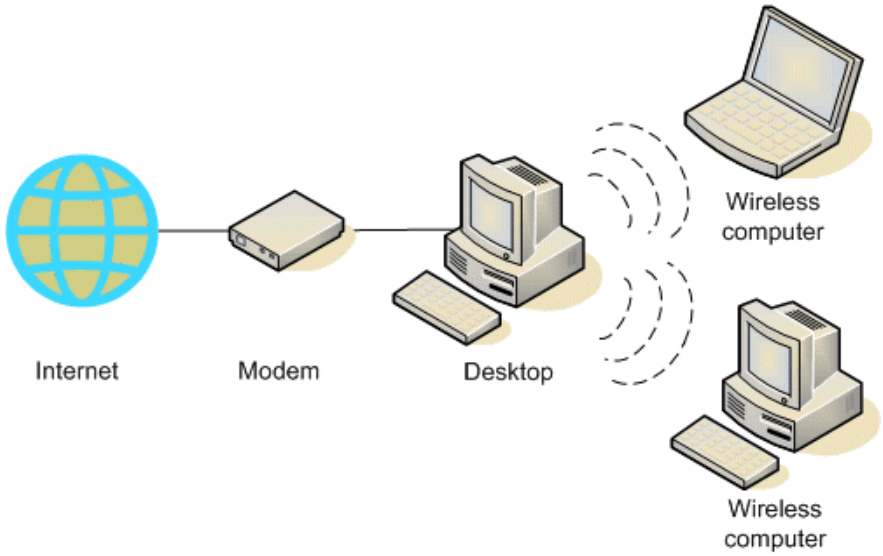

Figure 1.1. Ad hoc network operation for wireless devices without a central access point

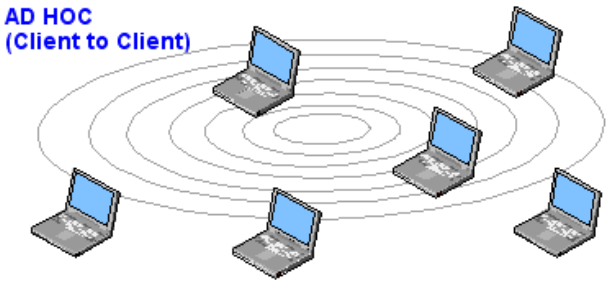

Figure 1.2. Peer-to-peer communication of ad hoc network clients when nodes are available within the range

An ad hoc network generally includes a small group of devices close to each other. With an increase in the number of devices, performance is compromised due to the decrease in

bandwidth per device. It is also difficult to maintain a large ad hoc network. In order to connect these ad hoc-connected computers to the Internet, special devices like a gateway are required [1]. Ad hoc networks are useful for creating and maintaining fast and cost-effective networks, for example, a wireless local area network (LAN). Ad hoc networks also work well as a temporary fallback mechanism, that is, if normally available infrastructure mode gear (access points or routers) stops functioning.

1.2 Applications of Ad Hoc Networks

In applications where a centralized node based system is not feasible, wireless ad hoc networks are found to be suitable due to their decentralized nature. The decentralized mode shows an improvement in the scalability of wireless ad hoc networks when compared to wireless managed networks. The practical limits of these networks must be considered when designing and deploying such networks.

Ad hoc networks have found increased usage because they require a very small amount of configuration and can be deployed quickly. Hence, ad hoc networks are found to be more suitable in emergencies like natural disasters. Due to the adaptive and dynamic nature, ad hoc networks can be formed quickly.

Wireless ad hoc networks can be further classified by their application as follows:

- Wireless mesh networks (WMNs) [2]
- Wireless sensor networks (WSNs) [2]
- Mobile ad hoc networks (MANETs) [3]

1.2.1 Wireless Mesh Networks

A wireless mesh network can be defined as a network of wireless nodes connected in a mesh style. Mesh routers, mesh clients and mesh gateways are the main components of such networks. Wireless devices such as laptops and cell phones fall in the category of mesh clients. The mesh routes the traffic through the gateways which may be connected to the Internet. The nodes in the wireless mesh networks operate under a certain radius. This range is known as a mesh cloud. Access to the mesh cloud depends on harmony between the various nodes. This forms a network known as a radio network due to the nature of the radio nodes. Mesh networks provide redundancy and reliability; in the case of one node becoming unavailable, the remaining nodes can still communicate with each other either by a direct connection or through intermediate nodes. Figure 1.3 illustrates an example of a wireless mesh network where there is no centralized node and the various buildings are connected in a mesh. When a single node stops responding, the other nodes can bypass it and communicate instead via the other nodes.

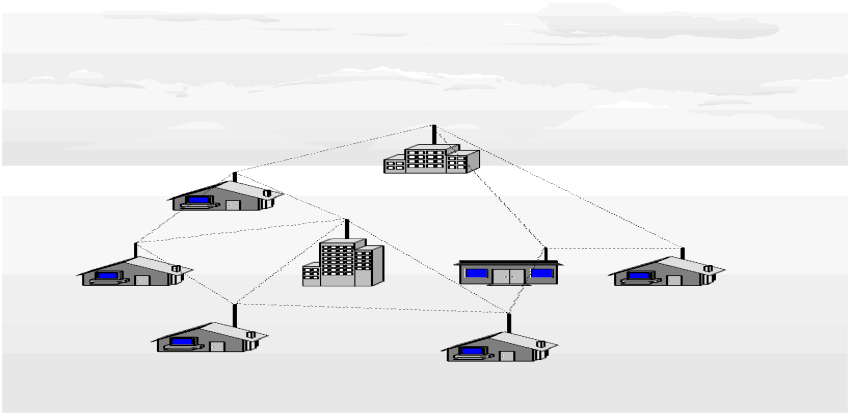

Figure 1.3. Illustration of wireless mesh network where each node must be connected (either directly or through intermediate nodes) to all other nodes

The nodes in a wireless mesh network can be stationary or mobile but often they are mobile. Also the routers in a mesh network are highly mobile. Typically they are not limited in resources and, unlike nodes can be used to perform many useful functions, such as using

dynamic routing protocols. This factor of resource constraint differentiates wireless mesh networks from ad hoc networks.

1.2.2 Wireless Sensor Networks

Wireless sensor networks are made up of sensors that are spread out spatially to monitor environmental or physical conditions, such as changes in temperature, noise or pressure. They are also used in military applications such as surveillance in battlefields. They were developed initially for the military but have found many industrial applications such as environmental monitoring. Other applications include traffic surveillance, weather monitoring and healthcare applications.

Each node in a wireless sensor network is equipped with a radio transceiver and a small micro controller in addition to other sensors to detect the signals. These sensors come in many sizes and forms ranging from the size of a grain to that of a shoebox. The cost of the production of these sensors is variable and ranges from a few dollars to a few hundred dollars. Size and cost are the main constraints, and research is being carried out in both areas to reduce these two constraints and facilitate their widespread use.

The sensor network, as shown in Figure 1.4, generally supports a multi-hop routing algorithm to route data from sensor nodes to a sink (gateway). Data gathering, data aggregation, and energy efficiency are active areas of research in WSNs.

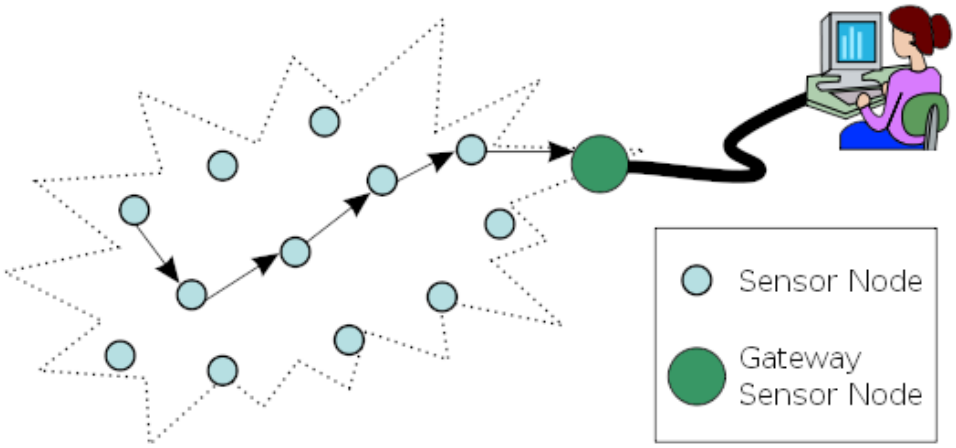

Figure 1.4. Example of communication in wireless sensor networks in which sensor nodes are dependent on a gateway or else communication fails

1.2.3 Mobile Ad hoc Networks

First used in the 1980s, wireless systems today are now in their third generation. The systems in use today give the user freedom to move around being able to communicate wirelessly using access points or a similar centralized support. In the future, there will be fast and easy deployment of wireless network, unlike the present systems, the efficiency of which affected in the absence of a permanent infrastructure. Recent advancements in this field have been mobile ad hoc systems an example of which is Bluetooth technology. Wireless networks are classified into two types: those that are infrastructure supported and those that exist without an infrastructure. Ad hoc networks do not require fixed and wired gateways and are considered infrastructure-less networks.

Ad hoc networks allow nodes to operate both as routers for all other nodes in the network and as an end system. These networks have control in the absence of a permanent infrastructure and offer quick deployment in most adverse conditions. In the case of fixed base stations being, a mobile host interacts with a base station available within a certain radius, known as the communication radius, and once the host starts moving geographically, it connects to another

base station, thus traversing from one base station to the other. This is known as handoff. A mobile ad hoc network consists of a group of mobile nodes that communicate mutually by wirelessly transmitting data packets. Ad hoc networks require no base stations or any kind of centralized infrastructure for administration, which facilitates the initial setup of requiring less effort and having a faster connection. Communication in a MANET is over a slow wireless link. Since the nodes are mobile, they make the network topology change rapidly, thus making it unpredictable over time. When a network is decentralized, a lot of the activity must be performed by the nodes. These include functions like delivering messages and discovering the topology. This is the reason for incorporating the routing functionality in these nodes. MANETs are self-configuring networks consisting of mobile routers connected wirelessly to form an arbitrary topology. The role of a router is performed by the nodes themselves, which are free to move around and thus manage themselves in an arbitrary fashion. This makes the network topology unpredictable and rapidly changing. This type of network can be connected to the Internet or made to operate alone.

Figure 1.5 illustrates the working of a MANET containing mobile nodes. The nodes configure themselves and establish a connection with the other nodes that are within their range of communication. Each mobile node in the MANET is independent and can move in any direction, thus, the links to other nodes in the network keep changing constantly. Each node must behave as an intermediate node by forwarding traffic that is not related to it, hence, performing the duties of a router. This is the main challenge in the configuration of a MANET to configure each node to behave as a router. Such networks once configured can operate independently or can be connected to the Internet.

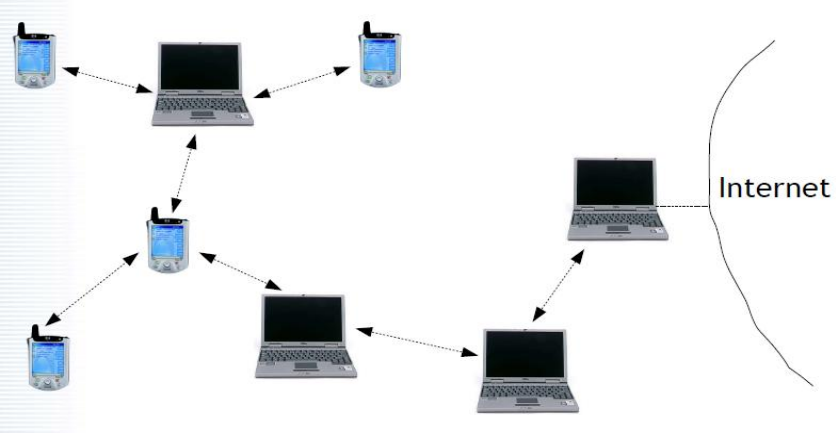

Figure 1.5. Example of communication in mobile ad hoc network without any base station

Mobile ad hoc networks are typically a combination of a wireless network's layer 3 routing feature and the ad hoc network's link-layer feature. Developments in the field of laptops and handheld devices that offer support to mobile wireless technologies have caused an increase in interest in 802.11/WiFi networks, which has led to a large effort and made MANETs a sought after research topic since the late 1990s.

An example of an ad hoc network consisting of four mobile nodes is shown in Figure 1.6. Here each node is taken to be in the transmission range of two other nodes, indicated with the help of circles around the nodes. Each node is in the range of the other two nodes but is out of the range of the third node. Hence, if two nodes that are not in the range of each other wish to communicate, they must use the assistance of another node to act as an intermediary node to forward the data on their part. In Figure 1.6, if node A wishes to send a data packet to node D, it must enlist node B (or C), as the intermediary node. Hence, node A should send the data first to node B (or C) and then the intermediary node can forward it to node D.

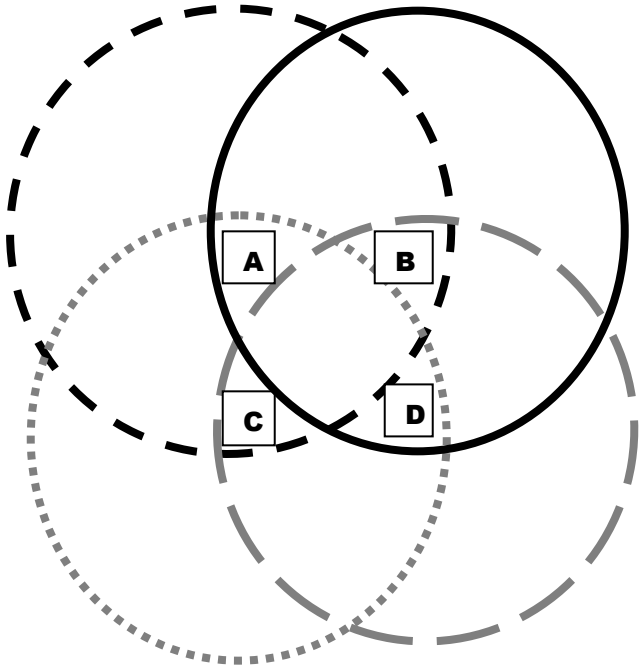

Figure1.6. Four-node mobile ad hoc network communication

In some error scenarios, part of the network becomes isolated and separate. This is known as network partitioning and is illustrated in Figure 1.7. In the event of network partitioning, nodes can exchange data between the nodes that are in the same partition but cannot communicate across partitions.

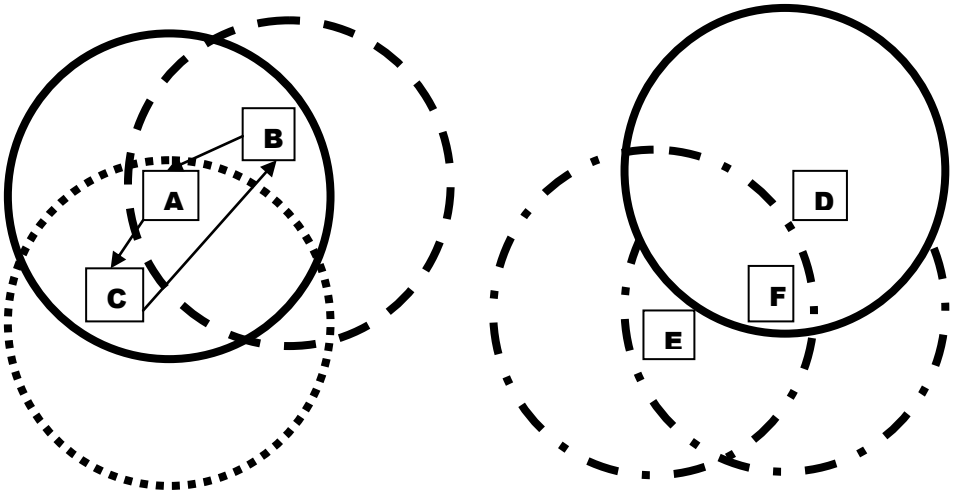

Figure 1.7. Network partitioning consisting of two partitions in MANETs

A common situation that occurs in wireless networks is shown in Figure 1.8. In this, node A has a very large range of transmission and hence can communicate with the other nodes effectively. However, node C has a very small range of communication and it must take node B as an intermediary node in order to return a data packet to node A.

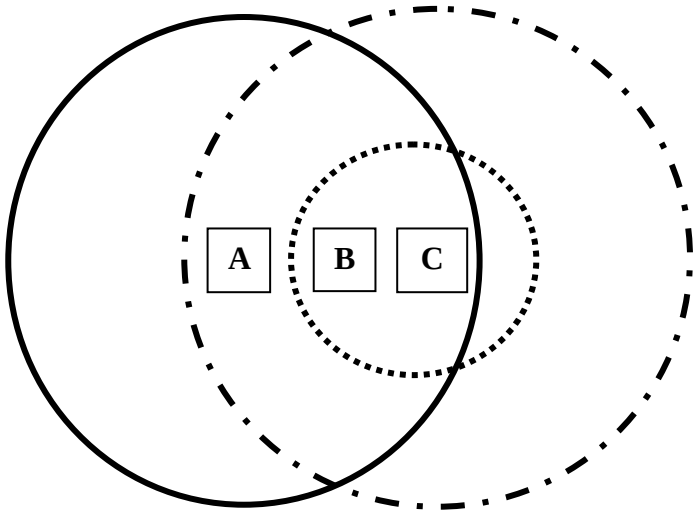

Figure 1.8. Unidirectional link in mobile ad hoc network when nodes are overheard

Many challenges face ad hoc networks. They perform multi-hop routing when required. The connectivity can be non-uniform and facilitates unidirectional links. They also allow for nodes to be mobile and continuously change their network location dynamically. These networks can get partitioned at times as well. Furthermore, the addition of new nodes to a network may occur unexpectedly, or a few existing nodes may leave the network suddenly. It is the goal of the ad hoc routing protocol to provide for connectivity of these nodes and maintain the network connectivity while overcoming these challenges.

1.3 Features of MANETs

In mobile ad hoc networks, uni-directional traffic is sent/received point to point while omni-directional traffic is broadcast traffic. Here the infrastructures are wireless transmitters and receivers. The wireless connectivity is always random and depends on the position of the nodes,

power levels, and channel interference level. At any given time, the topology changes are considered according to the transmitting and receiving parameters and the node's movement.

The means of communication is always wireless without any base station or access point. Here each node is self responsible for obtaining routing information about the destination to which it intends to send packets. MANETs serve the purpose of finding routes and maintaining routing tables. The nodes in mobile ad hoc networks act as both routers and hosts, where as in normal wireless networks, node refers to the host but not the router. Normal WiFi based wireless networks need a base station with which to communicate, which is not required in MANETs. MANETs have the flexibility to adapt to network changes that occur frequently in mobile ad hoc networks. MANETs operate under bandwidth constraints and capacity links that are variable. In mobile ad hoc networks, the energy-consuming operations, such as transmitting packets and controlling their speed, are confined and varied according to topology changes. Although nodes maintain routing tables, the route stability is unpredictable, leading to connection failure and packet drops, also known as low physical-layer security in the system. Dynamic topology allows the nodes to join and leave the network anytime, and no notification is expected from the nodes while leaving the network. Nodes must maintain persistent routing updates since the topology changes affect the routing path of the destination nodes.

1.4 Advantages and Limitations of MANETs

1.4.1 Types of MANETs

A common type of network used for communication between vehicles and for roadside assistance is the vehicular ad hoc network (VANET). During a vehicle-to-vehicle collision scenario, intelligent vehicular ad hoc network is effective in sensing the movements of vehicles when they are about to collide and can warn against a collision. Another common type of ad hoc

network used specifically to link mobile nodes is the Internet-based mobile ad hoc network (iMANET).

1.4.2 Advantages of MANETs

MANETS provide access to resources and data unaffected by geographic position, since the nodes are not dependent on any external single database system, and each node in the network is responsible for making the resources and data available to all other nodes in the system. The network topology in MANETs provides the convenience to set up the system at any place and time without the necessity of a base station or access points.

1.4.3 Limitations of MANETs

Since no specific data center is available for the nodes in a network, the resources such as bandwidth and network topology availability for mobile ad hoc nodes are very limited and the prevention of destruction or theft of data (known as physical security) is very low due to frequent topology changes. In mobile ad hoc networks, the inherent mutual trust and understanding of nodes are responsible for vulnerabilities to attacks since nodes cannot examine the authenticity [4, 12] of their neighboring nodes while accepting the information. Determining authenticity and authorization for MANETs is a very difficult task due to the dynamic nature of nodes and the lack of central monitoring points. Nodes communicate with all other neighboring nodes that are within the range of communication, and there is no provision to facilitate authorization. Detection of malicious nodes is critical due to constantly changing network topologies which may cause the misuse of resources available at benign nodes.

1.5 Contribution of This Thesis

The AODV routing protocol is an on-demand routing protocol for mobile ad hoc networks with the capability of facilitating a large number of mobile nodes in the network [3].

The protocol's algorithm creates routes between nodes only when the routes are requested by the source nodes, giving the network the flexibility to allow nodes to enter and leave the network at will. Unicast and multicast routing are supported and the routes remain active only during the actual transportation of data along the paths.

This research involves the use of the characteristics of the secure message transmission (SMT) protocol to reduce the overhead that occurs in the AODV routing protocol. The SMT protocol finds applicability in support of quality of service for real-time traffic. Under adverse conditions, in a network operating with the AODV routing protocol, there are malicious nodes. These adversaries drop packets, whick leads to their retransmission. During this process of retransmission, a few packets can be lost, which leads to delays, transmission overhead and routing overhead. By using the SMT protocol along with the AODV routing protocol, the retransmission of packets could be avoided, hence resulting in lower delays, lower transmission and routing overheads. These are the advantages of using the SMT protocol together with the AODV routing protocol as opposed to using the AODV routing protocol alone.

1.6 Organization of Thesis

The remainder of this thesis is organized as follows: Chapter 2 discusses the various routing protocols that are utilized in MANETs. Chapter 3 follows up with features of the AODV routing protocol. Chapter 4 provides an overview and describes the characteristics of the SMT protocol. Chapter 5 discusses performance improvements obtained by using the SMT protocol with the AODV routing protocol in the presence of adversaries (or malicious nodes). Chapter 6 concludes the thesis and discusses directions for future work.

CHAPTER 2

ROUTING PROTOCOLS

2.1 Definition of Routing Protocols

The process of data packet transfer from a source node to a destination node in a network is known as routing. The routing of data packets from source to destination nodes involves pre-computed routing paths and packet switching at each node along the path.

A routing protocol specifies how routers communicate with each other and disseminate information. This enables the routers to select routes between any two nodes on a computer network. The choice of the route is done according to the routing algorithm used. Every router has earlier knowledge only of the networks that are attached directly to it. A routing protocol shares this information throughout the network only after first sharing it among immediate neighbors. By this, the routers attain knowledge of the network topology.

Routing protocols use different kinds of metrics to determine the path for routing the packets to their destinations. Multiple paths can be selected by the routing algorithm. The routing algorithm finally selects the optimal path among them and stores in its routing table. The process of determining the optimal path and its maintenance in the routing table is known as path determination. The routing information varies according to the routing algorithms used.

The destination or the next-hop associations of the routing table notifies the router of the path for sending the packets to another router (namely the next hop) and on its way to the destination router. Routing is classified into two types: static and dynamic. Stating the routes manually (static) in the router is known as static routing. The network administrator writes the routing table for the static routing. The routing table in a static routing mechanism is constant and its state does not change with changes in network status, such as a destination being

active/passive. Dynamic routing involves improvement through routing protocols either interior or exterior. Dynamic routing depends on the state of the network. That is, the routing table could be affected by the active response of the destination.

2.2 Routing with Respect to MANETs

In MANETs, nodes use the same access wireless channel randomly, since the main goal of MANETs is to engage the nodes in multi-hop forwarding [5]. In a mobile ad hoc network, it is very necessary to have a routing procedure due to the lack of infrastructure support. Unlike wireless networks, the destination node could be out of range from a source node during packet transmission. In mobile ad hoc networks, due to frequent topology changes and no gateway router forwarding system, broadcasting is not allowed. Hence each node forwards data to the other nodes in the network. Lack of a broadcast feature also causes additional problems such as connectivity issues.

The routing protocols between pairs of nodes may face difficulties because these nodes can move in a random fashion and may leave or join the networks. This poses an issue of having an optimum route because the routes keep changing [2]. The ad hoc networks routing protocols can be categorized into three categories as listed below and represented in Figure 2.1:

1. Table Driven/Link State Protocols
2. On-Demand Protocols
3. Hybrid Protocols

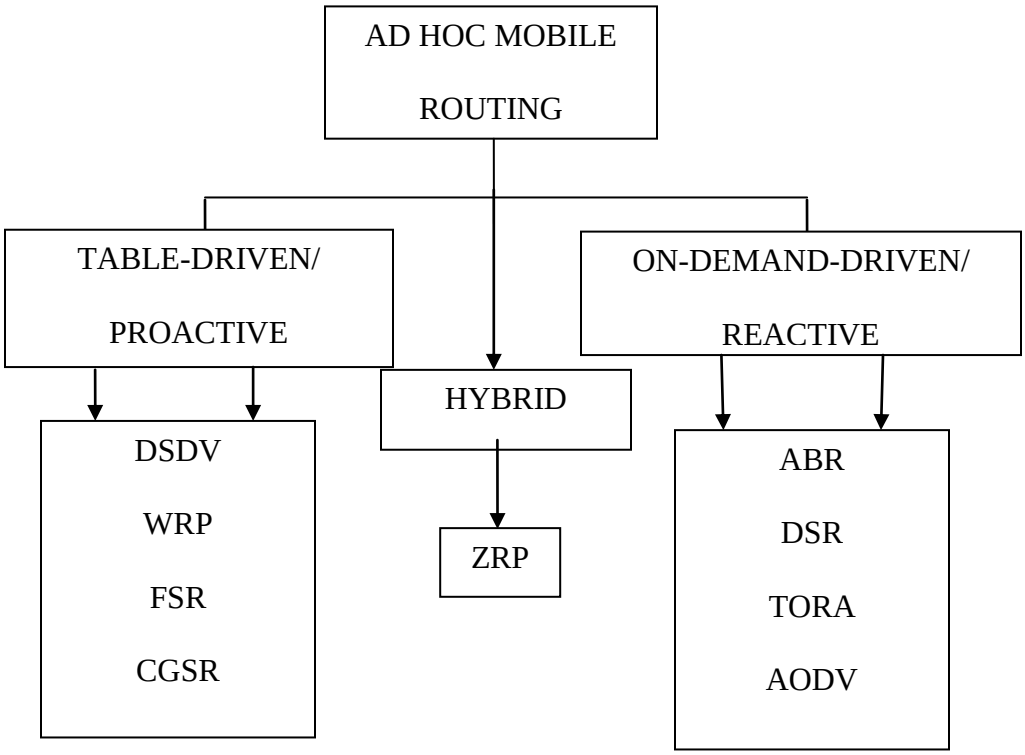

Figure 2.1. Ad hoc mobile routing protocols classification

2.2.1 Table-Driven Routing Protocols

Table-driven routing protocols are also known as proactive protocols or link-state routing protocols. These protocols work out the selection of routes in the background independent of traffic demands. The nodes store the location information of other nodes and use the information to move data among the nodes in the network. These protocols are susceptible to routing loops and are slow to converge. They always keep an overview of the network, which can prove to be a disadvantage due to the tendency to cause a change in the network even when it is not required. Table-driven protocols may not be suitable for routing in ad hoc networks due to their limited use of resources such as link bandwidth and power. An example of a table-driven protocol is the fisheye state routing (FSR) protocol.

Characteristics:

The link-state protocols select a router on each link for the flooding of topology information. In wireless ad hoc networks, packets can exit using the same interface; therefore, the approach for optimizing the flooding process is different. The protocols use hello messages at each node to discover the two-hop neighboring node information and a distributed selection of a set of multipoint relays (MPRs) is performed. The MPRs are selected such a way as to allow a path between each of its two-hop neighbors through a MPR. The topology control (TC) messages that contain the MPR selectors are then considered sources and forwarded from these MPRs. This feature makes the link-state protocol unique in a way that the path used for forwarding the TC messages is not a common one for all nodes but rather varies according to the source. Only the nodes that represent the MPR selectors are advertised instead of all the links of a node being advertised. This forms a subset of the link-state node information.

The protocols perform the topology flooding using a reliable algorithm since the link-state routing requires the synchronization of the topology database across the network.

Benefits:

Due to the fact that table-driven protocols are proactive, the routes within the network are tested and maintained before use. This helps in tabulating the routes within a standard table. This routing table can be particularly useful in the case of some networks and systems because it eliminates the need for route discovery delay caused while searching for a new route. The other rather important benefit with these table-driven protocols is routing overhead generated. Unlike other protocols, the routing overhead here does not increase with an increase in the number of routes in use but is generally greater than that of reactive protocol. By allowing a connection to the Internet or other networks in a MANET cloud, the Host and Network Association (HNA) messages can inject new routes into the system. Unlike reactive protocols, the timeout values and

validity information of network routes are contained within the messages and convey the information, which allows the use of differing timer values at different nodes.

Open Issues:

Due to the use of the flooding technique, there exists excessive traffic and control overhead in the network. Also, this flooding technique requires a lot of processor power, and therefore high power consumption is involved with these protocols.

2.2.2 On-Demand Routing Protocols

On-demand routing protocols are also known as reactive protocols. They establish routes between nodes only when the data packets have to be routed. They focus only on the routes being used instead of updating all the nodes that are possible. A route discovery is started only when the source node solicits information regarding a route. This process of route discovery checks all the nodes in the network until the route to the destination is found. These on-demand routing protocols are considered to be efficient during times when there is less frequent route discovery compared to data transfer. This is due to the reason that the traffic caused by this route discovery event is low when compared to the total bandwidth. Thus, these protocols are well suited for large networks with relatively low traffic and mobility. Dynamic source routing is an example of on-demand routing protocol.

Characteristics:

In on-demand routing protocols, the network is generally silent unless there is a connection requirement. When a connection is required, the node sends a connection broadcast with a request. The other nodes on the network transmit this message and keep a record of the node that they received this information. In turn this creates an enormous number of temporary routes which lead back to the node that sent the request. After receiving a message and

discovering the desired node, the node sends a message back through a temporary route. This process of gathering route information is known as "routing-by-rumor." The needy node (the node that requires the route) then uses the most efficient route with the least number of hops, and entries in the routing table that have not been used are recycled after a period of time. In the case of a link failure, a routing error is sent to the transmitting node. Then the process repeats.

Benefits:

A major benefit of on-demand routing protocols is the absence of extra traffic for communication along existing links, since the routing links are formed only during the time of sending traffic to the destination. Distance vector (DV) routing is simple and requires less memory and calculations due to the on-demand routing process. The fewer number of messages conserves the capacity of the network at the time of its initial setup. The creation of routes takes place only when desired by the source node, which is an efficient way to utilize bandwidth, but this in turn increases delay in routing process. Route maintenance is performed until the destination is not reachable from any path or if the route is not required.

Open Issues:

On-demand protocols suffer from slow convergence due to the "count-to-infinity" problem, since the routing is done by the "routing by rumor" process. Loops are created during node failure which causes network partition and/or congestion.

2.2.3 Hybrid Routing Protocols

A combination of on-demand routing protocols and table based routing protocols is used by hybrid routing protocols. These protocols make use of distance-vectors which provide precise metrics in order to establish the most efficient paths to destinations. Whenever there is a change in the topology of the network, distance vectors report the routing information. The number of

hops defines the zone radius which is used to measure the routing zone by each node. The nodes keep a record of the information about their routing zones. An example of hybrid routing protocols is the zone routing protocol (ZRP).

Benefits:

Precise path selection to all destinations is possible with hybrid routing protocols due to the separation of the entire network area into different zones. These zones help with efficient routing, even in the presence of a high number of nodes and heavy traffic.

Open Issues:

Zone selection in these protocols depends on the number of nodes per zone. Therefore, adding or removing nodes from the network causes reselection of the zones, leading to discrepancies in routing.

2.3 Properties of Ad Hoc Routing Protocols

Distributed network operation: Ad hoc protocols should be distributed and independent of a centralized controlling node. In an ad hoc environment, nodes can enter or leave at any given time and may partition the network due to their mobility. This is an important differentiating feature between ad hoc and stationary networks.

Loop free routing: In order to achieve optimal performance, ad hoc routing protocols ensure that the supplied routes are loop free thus preventing the bandwidth and processor consumption at nodes from being misused.

Demand based network operation: Ad hoc routing protocols are required to be reactive, which prevents the misuse of network resources. The main advantage of this property is that the protocols do not send periodic broadcast control information, they react only when needed.

Unidirectional link support: Ad hoc routing protocols should support unidirectional links, since the radio networks sometimes need unidirectional communication. The performance of the protocol is improved by bi-directional links.

Security: Ad hoc routing protocols should have some security features, which prevent impersonation attacks in a radio environment. In an ad hoc environment, distribution of public and private keys among the nodes is not possible, so authentication and encryption are not suitable for these networks.

Power conservation: Ad hoc routing protocols should support sleeping nodes, since in ad hoc networks, nodes can be laptops and thin clients such as PDA's, where battery power is limited and standby mode is used to save power.

Multiple routes: Multiple route usage can result in a reduced number of reactions due to changes in topology. The route discovery procedure for ad hoc protocols should store and be able to initiate alternate routes with the same hop count when the existing route becomes invalid.

Quality of Service Support: In order to support real time applications and traffic, it is important for ad hoc routing protocols to include quality of service in the routing protocol.

2.4 Issues in MANETs Routing

Asymmetric links: Unlike wired networks, ad hoc networks rely on asymmetric links due to mobile nodes and their constantly changing positions within the network. In wired networks, the route to destination is fixed and is through symmetric links.

Routing overhead: Some stale routes are generated leading to unnecessary routing overhead, due to frequent location change of nodes within the ad hoc network.

Interference: Transmission interference takes place when a node might over-hear the transmission of another node. In ad hoc networks this can cause the transmission process to be

corrupted and, depending on the transmission characteristics, the links may get established and torn down frequently.

Dynamic Topology: Since the network topology is agile, the mobility of nodes causes changes in medium characteristics which affect the routing tables and the routing algorithms every time. For instance, the routing table update takes place every 30 seconds in fixed networks and this update interval might be very low for ad hoc networks.

CHAPTER 3

AD HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTCOL

3.1 Introduction to AODV Routing Protocol

The first version of the AODV routing protocol was published in November 2001 by the Internet Engineering Task Force (IETF) community's MANET working group. This protocol belongs to the class of distance vector routing protocols. In a distance vector, each node has information about its neighboring node and is also aware of the costs required to reach them. A table with the information about all the nodes in a network and the next hop to the nodes with the distance is created and maintained by each node. The distance to a node is considered as infinity, in the event of the node being unreachable. The whole routing table is shared periodically among neighboring nodes which allows for the discovery of routes that can be used by making use of the neighboring node as the next hop.

The AODV protocol is an "on-demand routing protocol" with small delay. This implies that establishment of routes occurs only when there is a need to send packets. The AODV protocol can accommodate unicast broadcast and multicast communications. In case of multicast, the routes cannot support the movement of the mobile nodes. The five properties of the AODV protocol are: single path, state dependent, distributed, hop-by-hop, and deterministic [6].

The AODV protocol uses Internet protocol (IP) addresses as a unique identifying factor by setting 255.255.255.255 as the subnet mask. This allows it to also support aggregated networks. Only a single router serves as a default gateway. It is responsible for the total subnet's operation of the AODV protocol. It also maintains a sequence number. In the AODV protocol the routing table is expanded by a sequence number to every destination and by time-to-live

(TTL) for every entry. It is also expanded by routing flags, the interface, and a list of precursors and for outdated routes the last hop count is stored.

3.2 Route Maintenance

The three types of messages as defined by AODV are Route Errors (RERRs), Route Replies (RREPs) and the Route Requests (RREQs). These are received via UDP and the normal IP header process is applied. For example, the IP address of the requesting node is used as the originator IP address for all the messages. The IP limited broadcast address is used for broadcast messages (255.255.255.255). This shows that the messages are not just forwarded blindly. However, AODV requires that a few messages (such as RREQ) be disseminated widely, sometimes, throughout the whole ad hoc network. This dissemination range is indicated by the TTL in the IP.

The AODV protocol does not involve any overhead messages as long as valid routes exist between the endpoints of a communication connection. In the event of requiring a new route to a new destination, an RREQ is broadcasted by the node for finding the new route. The route is determined either when the RREQ reaches an intermediate node with a new "fresh enough" route to the destination or when it reaches the destination. "Fresh enough" denotes a route with a valid route entry to the destination, the sequence number of which is as large as the one in the RREQ. This route is made attainable by unicasting a RREP back to the RREQ's originator. Similarly, each node receiving such request caches a route back to the originator which enables the RREP to unicast from the destination along the originator path.

The link status of the next hop in active routes is monitored by the nodes. In the event of a line break in an active route, an RERR message is utilized for notifying the other nodes regarding the loss of the link. The destinations (probably subnets), which are not accessible via

the broken link are indicated by this RERR message. A “precursor list” is maintained at each node to enable the reporting mechanism. This list contains the IP address of the neighboring nodes which could possibly use it as a next hop to the destination. This information is easily obtained during the generation of the RREP message, which is sent to the nodes in the precursor list. The main goal of the originator of the RREQ is to solicit RREP information. However, this originator will include the neighboring node in the precursor list of the subnet route only if it receives the RREP with an optimal hop count. The precursor lists contain information for the subnet route but not specifically for any particular destination or IP address.

For a multicast IP address, a RREQ might be required in which the full processing of the message is not specified. For instance, the RREQ’s originator might have to follow a set of rules. However, it is required to allow the correct multicast operation by intermediate nodes which are not enabled as destination or originator nodes for the IP address and are not equipped for the multicast protocol processing. Hence, for such nodes that are not aware of multicast, the processing for a multicast IP as a destination IP is done in the same fashion as for any regular destination IP address.

Figure 3.1 depicts a route lookup session for the AODV protocol. Initially, node A does not have a route to node J. Node A tries to send traffic to node J, thus initiating a path. Node A floods all nodes in the network by broadcasting an RREQ. When H forwards the request to J, an RREP is generated at J. The RREP is then sent back to A as unicast, following the path H-G-D. The dotted lines specify either the sending or the receiving of packets between any two nodes.

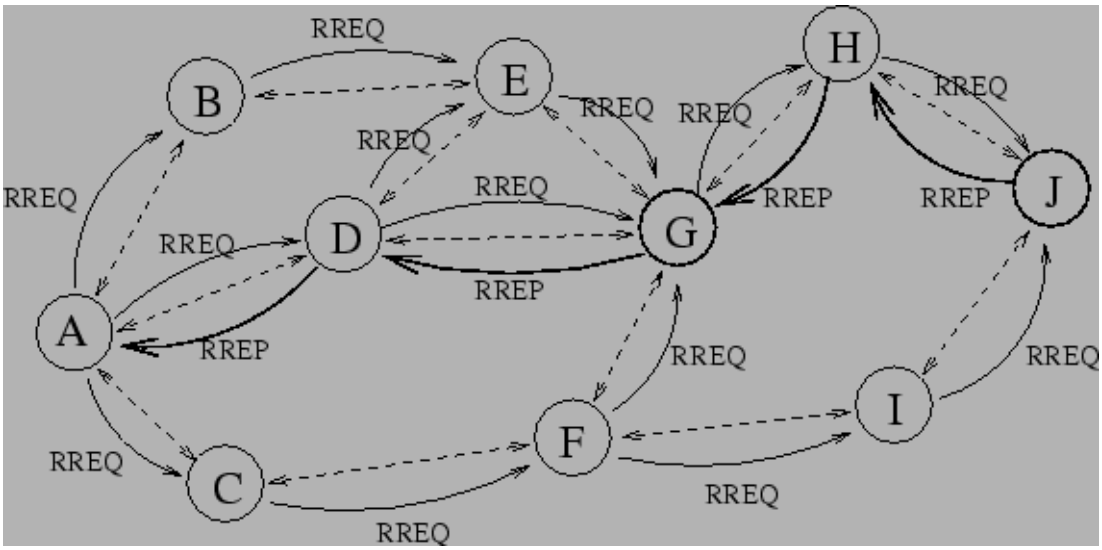

Figure 3.1. Possible path for route reply if A wishes to find route to J

3.3 Route Table of AODV Protocol

The AODV protocol deals with route table management. It is necessary to keep the table information even for short-lived routes. The AODV protocol uses various fields with each route table entry such as the following: (a) destination IP address, which is the 32-bit network layer address through which the destination node is identified; and (b) destination sequence number, which presents destination nodes with a chance to process or ignore the packet. If the sequence number of the arrived packet is less than or equal to the sequence number of the existing packet information in the route table, then arrived packet is ignored/dropped; else it is processed by the node. A destination sequence number flag is also included in the route table. There are three types of sequence number flags:

a. If the destination sequence number flag is marked as “valid”, then the packet information must be processed by the node

b. If the destination sequence number flag is marked as “invalid,” then it indicates that some error/interruption occurred while the packet was being transmitted, and these types of packets are ignored by the nodes.

c. If the destination sequence number flag is marked as “repairable,” the error that occurred is possible to repair, and the destination node sends the same information to the source node. Therefore, the source node again corrects the flag number and resends the packets.

The hop count is the column that provides information on the number of hops or nodes needed to reach the destination node. The next hop is the node which is directly connected to the source and this is the first hop to receive the packet when the source node starts transmitting. The list of precursors includes information about all the nodes that lie between the source and the destination. Lifetime is the time configured for the route information to stay in the route table if the route entry has not been used by the node for a certain period of time. This is also called as the expiration or deletion time of the route.

Managing the sequence number is important to avoid any routing loops. Even in the event of a link break when a node cannot be reached to relay the information of its sequence number. Thus, the destination becomes unreachable due to a deactivated link or a link break. In the occurrence of such conditions, the route is invalidated by using the sequence number which result in the route table entry being invalid.

3.4 Unicast Routing

In the case of unicast routing, three messages are available: route REQuest (RREQ), route REPly (RREP) and route ERRor (RERR). When a node requires sending a packet to a node that does not have a route available, an RREQ is broadcasted by the node to find a route. The

RREP has a unique identifier, a destination IP and a sequence number. The sequence number and the hop count are initialized with a zero. The sequence number flag is initially marked as valid. When a node receives a new RREQ, it sets a backward route to the sending node. In case the node does not know a route to the destination, the node re-broadcasts the updated RREQ after increasing the hop count. It creates an RREP, if the route to the destination is known.

Taking advantage of the reverse nodes, the RREQ is unicasted to the originator node. In the event of an RREP received by a node, the node checks if the hop-count for the emitter is lower than the value in its routing table or for the destination number, or if it is higher than the value in its routing table. If both conditions are false, then the node discards the packet. Otherwise, the routing table is updated, and if it is going someplace other than the destination, then the RREP is re-unicasted.

Link breakage is common in mobile network links. If a node discovers that the other nodes are unreachable, the node broadcasts a RERR with a list of the IP addresses and sequence numbers of the unreachable nodes and a few flags. A node that receives the RERR iterates the list to check if the next hop in its routing table contains any of the nodes in the list and updates its table accordingly. If the receiving node still maintains routes to unreachable nodes it broadcasts its own RERR containing this information.

The routes and link lifetime are extended by sending a data packet through hello messages. A hello message is an RERR that is valid only for neighbors. A node may periodically broadcast a hello message just to prevent neighboring nodes from assuming link breakages when there is no communication for a long time. In the case of a link breakage in an active route, a node could repair the route locally. To do this, the node sends a RREQ to discover a new route to the destination on the link breakage side. Another special packet, a route reply-acknowledge

(RREP-ACK) is used for unreliable or unidirectional links. Also some other special mechanisms are used like precursors to track the list of active routes for use in an RERR emission.

3.5 Multicast Routing

Multicast routing is one of the most important advantages of the AODV protocol. The IP addresses and the sequence numbers of the group are stored in the multicast routing table. The hop count and the IP address of the leader are also stored. By sending an RREQ to the group address along with a join flag set, a node can join the multicast group. Any node that receives the RREQ can reply with a RREP. In this manner, the requester receives several RREPs and selects the one that is the shortest distance from the group. For activating the branch, a multicast activation (MACT) message is sent to the chosen tree. In the event of a receiver not receiving a RREP, the node assumes that the multicast tree is non-existent for the group member. Thus, it becomes the leader of the group. A multicast RREP may contain the group leader's IP address and the hop count to the next group member. The leader of the group periodically broadcasts a hello message (RREP), thus increments the sequence number each time.

Two partitioned group trees may need to be linked in the event of the connection of two network segments. Every member of the group that receives two group hello messages from different leaders would detect a tree connection. The node then sends an RREQ with the repair flag set to the group. If a node in the group tree does not receive any group hello or other group message it must repair the group tree with a RREQ. Also, it should ensure that a RREP from a node in its own sub-tree is not chosen. If a group member (a leaf) is willing to leave the group, it can do so by pruning the branch using a MACT and the prune flag set. In the case of the group member not being a leaf, the member must continue as a tree member.

3.6 Security in AODV Routing protocol

Security is very important in mobile communication. Impersonation attacks can be easily carried out due to the AODV protocol having no specific security mechanisms defined. In order to prevent this attack, authentication is required, for example with public key authentication (PKA). Messages can easily be intercepted. In order to prevent this one can cipher them, for example with a public key. Standard IP security protocols like Internet protocol security (IPsec) should not be used since its authentication is based on the node's IP addresses and is a pre-determined security association. However, mobile AODV protocol nodes cannot be expected to have a pre-assumed unique address.

3.7 Implementation of AODV Routing Protocol

There are two types of AODV routing protocol implementations: user-space daemons and kernel modules. The first requires maintaining a routing table and was first implemented [6] in the ad hoc implementation by Lilieblad et al. running on a Linux 2.2 kernel, but this does not support multicast. The University of Uppsala also published a user-space daemon implementation called the AODV-University of Uppsala (AODV-UU), which runs on Linux with a 2.4 kernel [7]. The newest daemon MANET was published on the April 2, 2002 [5] by the University of California, Santa Barbara, also running on a Linux with a 2.4 kernel. The only kernel implementation was done by the National Institute of Standards and Technology (NIST), Wireless Communications Technologies Group running on a Linux with a 2.4 kernel. It is very fast and efficient reaching the best performance of all implementations [8].

3.8 Characteristics of AODV Routing Protocol

A few characteristics of the AODV protocol are discussed in this section. On-demand routing is responsible for discovering hops, either in broadcast mode or in non-broadcast mode.

Unlike link-state routing protocols, the distance vector protocol supports all three- unicast, multicast, and broadcast. It is not necessary to have an additional protocol in the AODV protocol environment to obtain a loop free network. The AODV routing protocol itself has an added feature of including a topology database table to ensure that no redundant paths are formed. Quick aging is one of the characteristics of the AODV protocol and is responsible for the timeout of route entries in the database. Although quick aging makes the communication reliable, it is because of this feature that the AODV protocol faces issues like unnecessary delays to find a new path to the destination. Distributed routing is a type of route-by-rumor procedure in wired networks. The node receives some information about the destination from the neighbor and with that information it forwards traffic in the manner specified by this neighbor. Although the protocol does not have destination information, it is certain about the next-hop information which could take care of the path for the traffic to its destination and the next hop follows the same. This is known as hop-by-hop routing. The AODV protocol is deterministic in nature, that is, in a given AODV protocol environment, the routes between a pair of nodes are pre-programmed or determined in advance to transmission. Nodes learn routes and select a single best route to each destination. These protocols are incapable of load balancing traffic. Single-path interconnected networks are not fault tolerant.

3.9 Advantages of AODV Routing Protocol

The AODV protocol does not require a central administrative system for handling the routing process. It is a flat routing protocol, whereby routes are constituted on demand. The sequence numbers are utilized for finding the latest route to destination. The AODV protocol reduces the overhead of control traffic messages at the cost of an increase in latency in route

discovery. This has a relatively low connection setup delay. The AODV protocol is loop free and avoids the count-to-infinity problem by utilizing sequence numbers.

3.10 Disadvantages of AODV Routing Protocol

Inconsistent routes may occur due to the source sequence number. If the value of the source sequence number is stale at the source and the intermediate routes contain a higher (but old) destination sequence number, then heavy control overhead may be caused if multiple RREP packets are sent in response to a single RREQ packet. The periodic beaconing leads to unnecessary bandwidth consumption which leads to congestion and packet drops in the network.

CHAPTER 4

SECURE MESSAGE TRANSMISSION PROTOCOL

4.1 Introduction to Secure Message Transmission Protocol

Data transmission and route discovery are the two stages involved in mobile ad hoc network communications. When considering an adverse environment, these two stages are prone to a wide variety of attacks. The attacker may cause a disruption in the discovery of routes by an impersonation of the destination, or by sending old and corrupted information. The attacker may also broadcast control traffic that is forged. The adversaries, through these various techniques cause an obstruction in the movement of correct route control traffic and negatively impact the topological knowledge of the amiable nodes. These attackers can also cause a disturbance in the phase of data transmission which leads to a measurable loss of data due to forged redirecting, the addition of impersonated data packets or by causing a drop in data traffic and data packets.

In order to provide an overall security, both phases involved in MANET communication must be protected. Secure routing protocols do provide the accuracy of any given topology but cannot guarantee the security for a continuous flow of data transmission. This is due to the fact that the attackers can place themselves on the nodes in use and follow the route discovery. They can then disrupt the data in transmission in a random manner, thus leading to a disturbance in the operation of the overall network.

A few of the upper-layer mechanisms in the MANET routing protocols, such as reliable transport protocols or acknowledged routing, do not have the capacity to cope with the adverse effects and disturbances of the data transmission. The communication nodes under them can be misled for a long period of time, under the assumption that there is an undisrupted flow of data even when the communication has ceased to flow.

There are many options to counter these adversaries. Cryptographically protecting and authenticating the traffic and control messages is a viable option. To achieve this, the nodes need a way of building required trust with neighboring nodes that forward the data. Even with such an implementation, the cryptographic protection would fail to protect against the denial of service attacks, when attackers reject the packets of data. The SMT protocol is an end-to-end secured data transmission protocol that is suited for the MANET environment. It defends the communication among nodes in a frequently changing network even when attackers that disrupt the behavior are present. It works through a combination of four features: (a) an end-to-end secure and sound feedback system, (b) ability to use multiple paths at the same time, (c) propagation of data transmitted, and (d) adaptation to frequently changing network conditions. Thus, the SMT protocol can detect and withstand transmissions under adverse conditions while coping and adapting itself to the network in order to provide a secure data transmission that avoids high delays.

The main aim of the SMT protocol is to provide security to the route discovery phase; however, the SMT protocol cannot discover routes. Its aim is to achieve secure data forwarding and this takes place after the discovery of routes. That is, the SMT protocol operates under the assumption that there is a fixed protocol that has taken care of the discovery of routes in the ad hoc network. Since the routes may contain malicious nodes, the aim of the SMT protocol is to provide a safe routing of data under adverse conditions.

4.2 Overview of SMT

SMT protocol operation requires association between the two end nodes, that is, the source and the destination. Because this pair of nodes is responsible for engaging the secure communication method, they have to be able to authenticate each other. This can be

accomplished by knowing the public key at the other end. It should be noted that none of the other nodes in the network require any association with the end nodes. Hence, SMT does not need any safety operations at these transitional nodes.

In the case of the SMT protocol, at any given instance, the two end nodes employ a set of distinct, node disjoint paths that are valid at that time. These paths are referred to as active path set (APS). The source first evokes the route discovery and updates its network topology view, thus determining the initial APS for communication with the destination.

Since the set of routes has been established, the source disperses each message into a number of pieces. The dispersion at the source is based on an algorithm. The algorithm introduces redundancy and encodes the messages. On receiving the dispersed message at the destination, the message is reconstructed only if an adequate number of pieces are received. Even with a few missing pieces of messages caused by the malicious nodes, the message can still be reconstructed at the destination.

The dispersed pieces of the message are transmitted through a different route with a MAC (Message Authentication Code) which enables the destination to verify the authenticity of its origin. After the destination validates the authenticity of the incoming message, it sends an acknowledgement across a feedback route back to the source.

The mechanism that the destination uses is secure and fault tolerant as well as cryptographically protected. This ensures that the source receives only authentic feedback from the destination that specifies the pieces of messages that were received by the destination. A route is deemed to be operational when the loop is successfully completed. A failure in the mechanism is an indication of the route being compromised.

4.3 SMT Protocol Operation

The source constantly keeps updating the ratings of the different paths with each transmission across the APS. For each piece that is transmitted, the corresponding rating of the path is either decreased or increased. Once a path fails, the path is discarded and precautions are taken to avoid using the same path again. The assessment of the paths is done continuously and the operation adapts itself according to the feedback it receives. Thus the paths remain active even in adverse environments.

The destination can reconstruct the message only if it receives an adequate number of pieces of the transmitted message. If the message cannot be reconstructed, the destination waits for the remaining pieces, which are then retransmitted by the source. These retransmissions are limited to a maximum of $\text{Retry}_{\text{max}}$ codes per message.

Figure 4.1 shows an illustration of a single message being transmitted. As shown, the source disperses the message in four packets. Any three of these four transmitted packets are sufficient for the reconstruction of the transmitted message. The four packets are transmitted over four distinct and disjoint paths, and two of the four are successfully transmitted. The remaining two packets are not delivered due to the presence of malicious nodes. This is shown as the packet that is dropped and the other is represented by the dashed arrow.

Once the receiver receives the information from the first packet, it waits for the remaining packets and sets a reception timer. Once the fourth packet is received, the cryptographic integrity checks the packet for tampering and the packet is rejected. Once the timer expires, the receiver sends an acknowledgement reporting that the two packets have been received successfully. The acknowledgement is sent across the two operational paths.

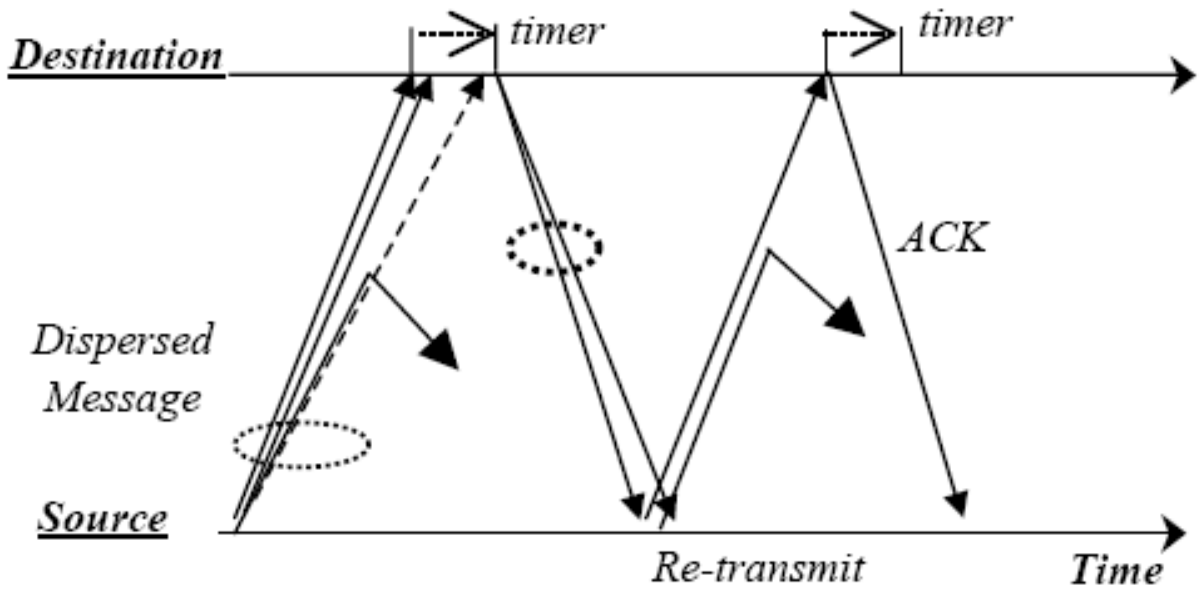

Figure 4.1. Operation of SMT protocol

The source only requires receiving one validated acknowledgement and ignores the remaining duplicates. The two paths that failed are ignored and discarded. The two missing pieces are again retransmitted over other paths. If one packet is now lost, for example, due to some malicious node or a path breakage, the receiver sends an acknowledgement of successfully receiving the other packet immediately before the timer expires, since the destination has received a sufficient number of packets. After the transmission of the first packet, the sender also sets a retransmission timer, which serves the purpose of accounting for total lost message pieces.

4.4 Characteristics of SMT Protocol

An end-to-end secure and robust feedback mechanism of the SMT protocol provides feedback when any route fails. Dispersion of transmitted data is nothing but spreading the data through multiple paths and also the simultaneous usage of multiple paths. Adaptation to network changing conditions is one of the most important features of the SMT protocol which helps to notify the nodes about the route failure due to physical breakage or malicious nodes.

CHAPTER 5

AD HOC ON-DEMAND DISTANCE VECTOR PROTOCOL WITH SECURE MESSAGE TRANSMISSION

5.1 Introduction

General objectives can be outlined to generate a simulation environment that could be used for analysis of the AODV protocol with the SMT protocol. The proposed protocol can, successfully cope with a high number of adversaries, while operating only in an end-to-end environment.

5.1.1 Contribution of This Thesis

In this thesis, the following protocols are evaluated: (a) AODV-data-forwarding protocol which employs very little security mechanism to protect data transmissions (b) AODV protocol with the SMT protocol. In these two cases, it is assumed that the route discovery is secured, that is, the correctness of the discovered connectivity information is guaranteed. It is found that the AODV protocol together with the SMT protocol can deliver successfully more than twice the number of packets delivered by a normal routing protocol, i.e., the AODV protocol that secures only the route discovery phase but not the data-forwarding phase. Moreover, it was also found that the AODV protocol with the SMT protocol is successful in delivering data with low end-to-end delay, low routing overhead, and limited transmission overhead, when compared to the native AODV protocol.

The AODV protocol is the limiting case of the AODV protocol with the SMT protocol without the dispersion of outgoing messages and the use of a single path for each message transmission. The AODV protocol is equipped with the same end-to-end feedback and fault detection mechanisms as the SMT protocol. The AODV protocol alone also re-transmits each

failed message $Retry_{max}$ times, and provides data integrity, authenticity, and replay protection, just as the AODV protocol with the SMT protocol does, and selects the shortest path in hops. The AODV protocol determines, utilizes, and maintains a single path only. Once the utilized path is deemed failed, a new route discovery may be needed in order to determine a new route which is not necessary in the AODV protocol together with the SMT protocol.

5.2 Simulators

This section explains the most common network simulator used, the chosen platform for the implementation of the protocol, and the actual simulation required for this thesis.

5.2.1 Network Simulator – NS-2

Network simulator 2 (NS-2) is a discrete event simulator used in networking research projects. The Network Simulator provides support for simulating the transmission control protocol (TCP), a layer 4 connection oriented protocol under wired and wireless networks. Two simulation tools are used: the network simulator (NS) supports most protocols that are commonly used, and the network animator (nam) is used for simulation visualization. It was originally developed by the University of California and Visvesvaraya National Institute of Technology (VNIT) project. The simulator was later extended by Carnegie Melon University to simulate ad hoc networks. Features of ad hoc network such as the use of mobile hosts for cellular networks and the use of multiple paths for routing packets make a perfect scenario for simulation using NS-2. The C++ and OTcl languages are generally used for NS-2 programming. NS-2 is an object oriented simulator. In both the OTcl and C++ interpreters, support for class hierarchy is provided by the simulator. There is ample reason to use two different programming languages. For configurations and programs that require frequent changes, OTcl is suitable, whereas programs that require high speed execution are programmed using C++. NS-2 has a wide range

of applications. Along with providing support to the most commonly used Internet protocols, it also allows users to extend the implementation to their own design of protocols. The NS-2 also provides superior trace functionalities which play a major role in this project since there is a need for information to be recorded for the analysis. The NS-2 code is available for download and can be compiled for various platforms [9].

5.3 Mobility Models

The protocol needs to be tested under realistic conditions in order to obtain a good evaluation of its performance in an ad-hoc network. The conditions should include the mobile node movements. Different models are discussed below. In this thesis, the random waypoint model was utilized.

5.3.1 Random Walk Mobility Model

The model is based on a selection of speeds and directions randomly. A node selects a speed in the range of 0 and $V_{max.}$ The direction is selected between (0, 0) and (0, 2) towards north. The speed and direction are recalculated either after a given amount of time has elapsed or a certain distance is covered. Since, this model does not have any memory, the directions and speeds that occur later are in no way dependent on the elapsed speeds or directions. This feature may result in a few unrealistic moves by the nodes such as sudden halts or sharp movements. Depending upon the distance or time, the nodes may get restricted to a small area of simulation.

5.3.2 Random Waypoint Mobility Model

The movement of a mobile node occurs after a pre-determined pause-time. A random speed and a destination are selected at the end of the pause time. Upon reaching the destination, the node waits for the pause time again. Then it selects a new speed and waypoint (reference point). At the start, the mobile nodes are scattered. The scattered distribution of the nodes does

not represent their final distribution caused by their movement. At the start, a certain amount of simulation time is discarded, and then the results of the simulation are recorded. This is to ensure a random configuration initially. The Random Waypoint Mobility Model has been found to be used extensively in studies that include the simulation of MANETs. It is desirable to stabilize the average speed and prevent it from changing constantly with time. A comparison is desired between the mobile ad hoc routing protocols at various speeds. Since the speeds are uniformly chosen from 0 to V_{max}, the expected average is about half the maximum. If the average speed is not reached during the simulations, it could lead to an error in the results obtained. The explanation for this is as follows: the node selects the speed and the destination. The node maintains the speed (selected previously) until it reaches the destination. Depending on the speed selected and the destination, the node might travel for a longer or a shorter period. For example, if the node selects a high speed close to V_{max} and a destination that is far, the travel time will be shorter than the time if it had selected a speed close to 0. The node, after a certain period of time, would have travelled at a lower speed than at a higher speed, which leads to the average speed close to 0m/s. This problem can be resolved by selecting V_{min} equal to 1m/s rather than 0m/s. This results in a stabilization of the average speed after a certain period of time. The value of the average speed can be determined to be ½* (V_{min} + V_{max}).

5.3.3 Random Direction Mobility Model

A density wave is considered to be a clustering of nodes in a single area of the simulation [10]. For a reduction in density waves, the random waypoint model was devised. In this model, the probability of a node travelling through the center and then selecting an area close to the waypoint is high. The mobile node selects a direction for travel and goes towards the edge of the simulation area. In the mean time, if the boundary is reached, the node chooses a new direction

after pausing for a pre-determined period of time. This pausing of the node causes an increase in the hop time (time taken by a packet to travel between two nodes) for the mobility model. In research conducted at Carnegie-Melon University, a model to support the simulation of multi-hop networks along with the information and data was developed. The characteristics of this model are similar to the characteristics of a Lucent WaveLAN [11]. The WaveLAN is designed as a shared-media radio with a radio range of approximately 250 m and a bit-rate of 2 Mbps.

5.4 Traffic and Mobility Models

Sources for constant bit rate (CBR) traffic are also included in the configuration. The source and destination pairs are spread in a sporadic fashion throughout the network. Varying load in the network is attained by varying the sending rate and the number of pairs of sources and destinations. The traffic and mobility models use the random waypoint in a rectangular field of operation whose configurations are 520 m x 520 m with a total of 100 nodes. Now, each packet starts travelling from any random source towards a random node at a randomly chosen speed. Upon reaching the destination, the node selects another destination at random after a certain pre specified pause time. The pause may vary from one node to the other and it affects the relative speed of the nodes. Simulations were run for 200 seconds.

The buffer selected by the routing protocols that use this random direction mobility model contains up to 64 packets. These include all the data packets that are waiting to find a route since the start of the route discovery. If a packet waits in the buffer for more than 30 s, the packet is dropped; this prevents the indefinite buildup of packets in the buffer. Until the MAC layer is ready for transmission, all the data and routing information are put on hold in an interface. The interface queue is served first in first out (FIFO) and has a limit on the number of packets to 50.

5.5 Simulation Setup

The random waypoint mobility model was used in this thesis because of its ability to replicate the random movement of nodes in a network. This same model was used for all simulations. One hundred nodes were used, and a 2 s pause time was determined. The maximum speed V_{max} was set at 20 m/s, while the numbers of malicious nodes were changed as 0, 10, 20, 30, 40, and 50.

A few simulation parameters that used assigned values are shown in Table 5.1.

TABLE 5.1

SIMULATION PARAMETERS

Parameter	Value
Number of Nodes	100
Simulation Time	200 s
Pause Time	2 ms
Environment Size	520 x 520
Transmission Range	100 m
Traffic Size	CBR
Packet Size	512 bytes
Packet Rate	4 packets/s
Maximum Speed	20 m/s
Queue Length	100
Simulator	ns-2.29
Mobility Model	Random Waypoint
Antenna Type	Omni-Directional

5.6 Performance Metrics

The AODV protocol was compared with the proposed protocol (AODV protocol in combination with SMT protocol) for four different performance criteria namely, end-to-end delay, packet delivery ratio (PDR), throughput, and routing load. Multiple experiments were conducted and averages of the results are displayed in tables 5.1 and 5.2.

The formulae used in the simulation include the following:

PDR=AGT rcvd/AGT sent

Routing load = RTR sent/AGT rcvd

Throughput = AGT rcvd/sim.time

Agent packets (AGT) refer to the control packets which are sent periodically between the nodes to check the availability of the connection.

Routing packets (RTR) are network layer packets. These are the actual data packets which are communicated between the nodes.

5.6.1 End-to-End Delay

End-to-end delay can be defined as the time the node takes to send a packet from a source to a destination in a network. Figure 5.1 plots the end-to-end delay for the AODV protocol and the AODV protocol in combination with the SMT protocol for various choices of malicious nodes. It is observed that the end-to-end delays are up to 43% lower when using the AODV protocol with the SMT protocol as compared to the AODV protocol alone.

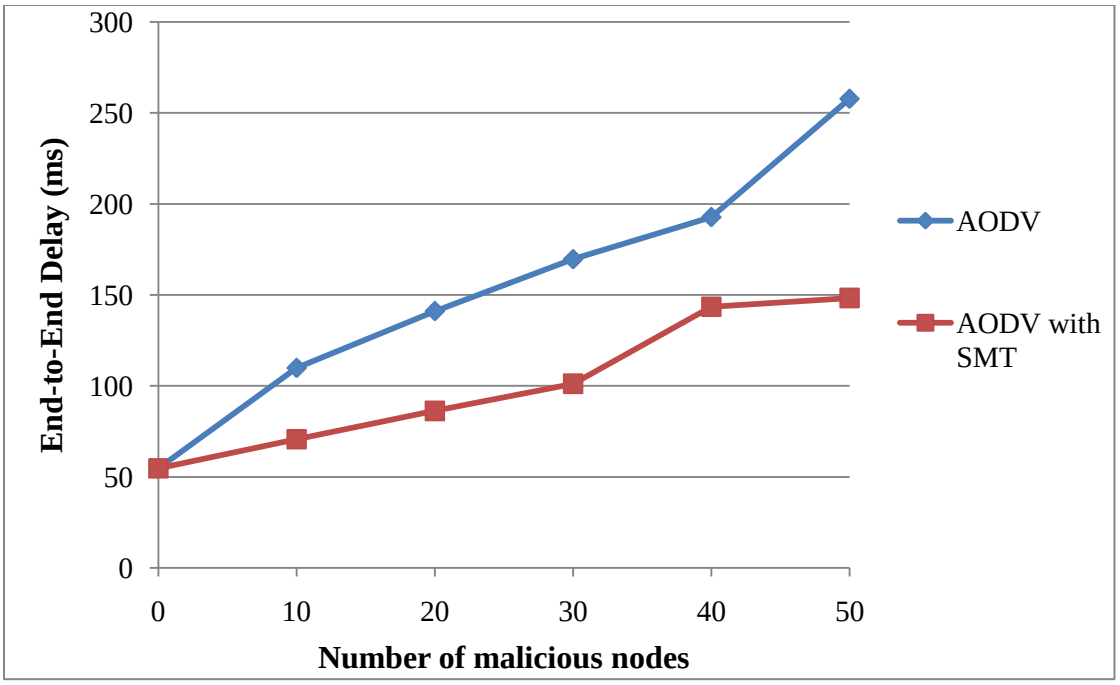

Figure 5.1. End-to-end delay vs. number of malicious nodes

5.6.2 Packet Delivery Ratio

The packet delivery ratio (PDR) is the ratio of delivered destination data packets to the number of packets that are generated at the CBR sources. As seen in Figure 5.2, the AODV protocol together with the SMT protocol delivers 9% more data packets, even when half of the nodes are malicious, when compared to the AODV protocol alone.

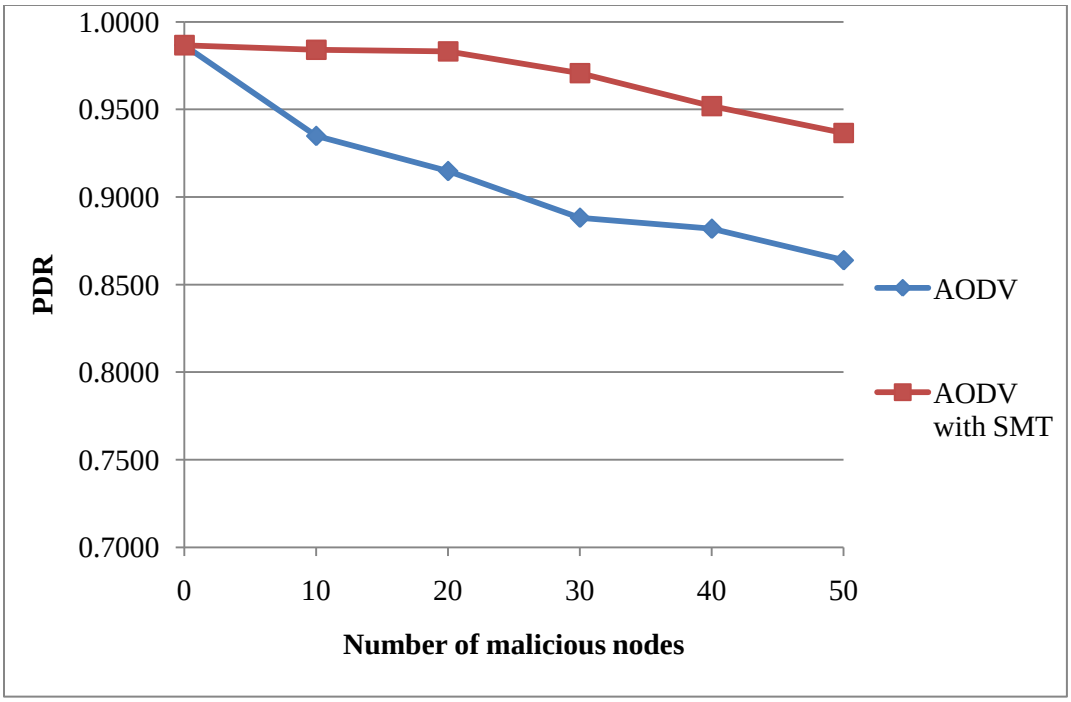

Figure 5.2. PDR vs. number of malicious nodes

5.6.3 Throughput

Throughput is represented in two different ways. One is the percentage measure of the packet delivery, which is calculated using the number of data packets sent and received. The other is the amount of data transfer that has occurred in a given interval which is expressed in kilobits per second (kb/s). Figure 5.3 plots the throughput (in terms of kb/s) vs. the number of malicious nodes. As shown throughput increases by as much as 12% when using the AODV protocol together with the SMT protocol in comparison to just the normal AODV protocol. Throughput is almost constant throughout the experiments since AODV with SMT has only 2% packet drops even in adverse conditions. Due to message dispersion, the alternate paths that are stored in the route cache can be used immediately. This means that there is no need to discover new routes constantly and hence the AODV protocol with the SMT protocol gives a constant throughput even in adverse conditions.

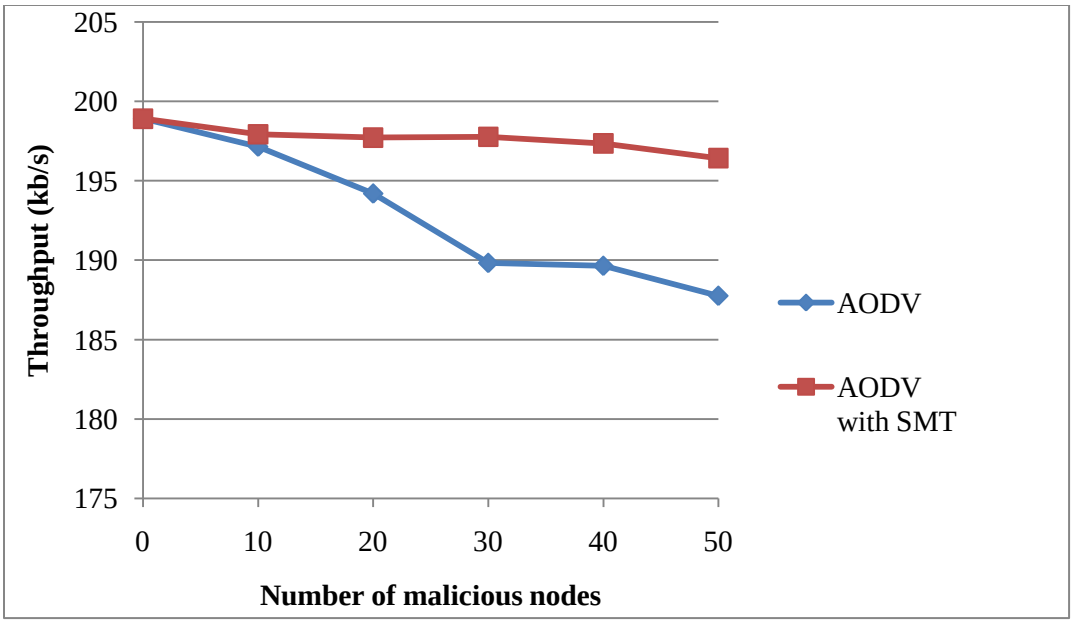

Figure 5.3. Throughput vs. Number of Malicious Nodes

5.6.4 Routing Load

Routing overhead of a reactive protocol is the total number of control packets launched in the network by the protocol in response to a route request (RREQ) message, limited to an arbitrary number of hops from the source node.

Figure 5.4 plots the routing load vs. the number of malicious nodes. It is observed that the AODV protocol with the SMT protocol imposes up to 14% less routing overhead in comparison to the normal AODV protocol. Due to the presence of malicious nodes, the normal AODV protocol has to constantly discover new routes thus leading to an increase in the routing overhead. The AODV protocol with the SMT protocol has secondary routes stored in the route table, thus maintaining the routing load as constant.

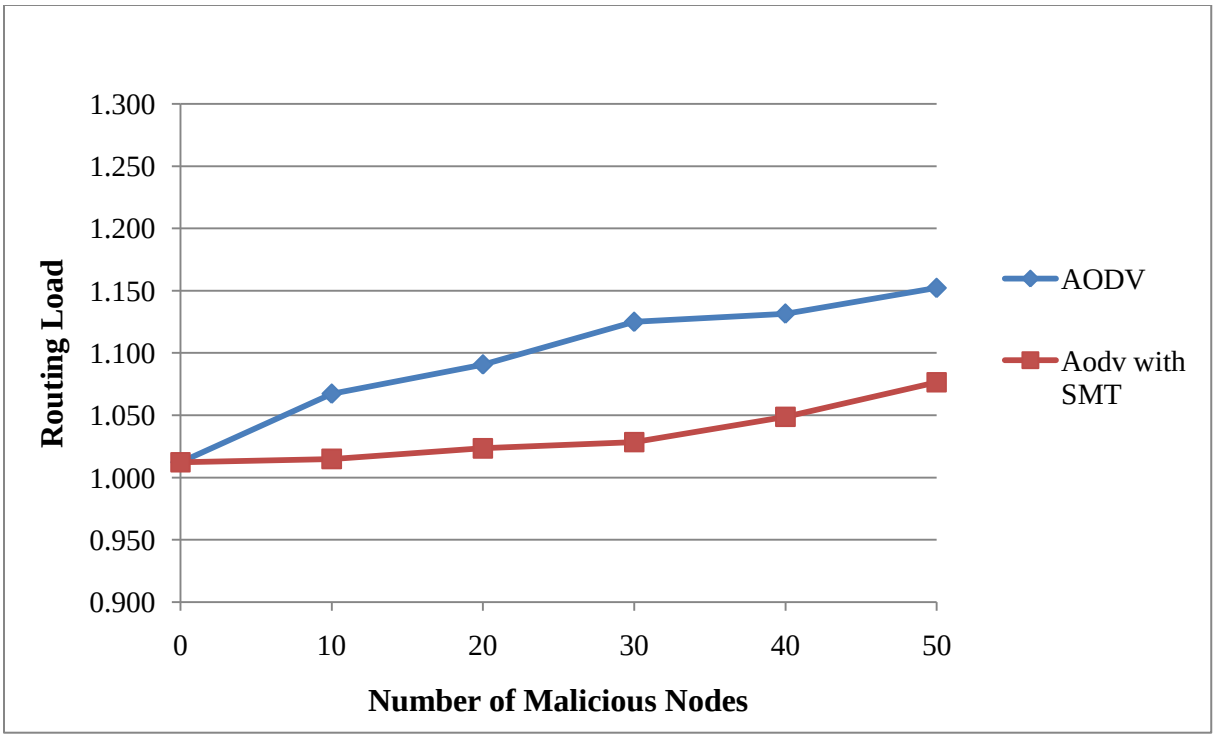

Figure 5.4. Routing Load vs. Number of Malicious Nodes

Tables 5.2 and 5.3 show the performance evaluated for the AODV protocol and the AODV protocol in combination with the SMT protocol, respectively.

TABLE 5.2

PERFORMANCE EVALUATED FOR PROTOCOL AODV

No of Malicious Nodes	AGT - SENT		AGT - RECEIVED		RTR - SENT		PDR	ROUTING LOAD	THROUGHPUT (kb/s)	End-to-End Delay (ms)
	Kb	PACKETS	Kb	PACKETS	Kb	PACKETS				
0	40317	9843	39780	9712	40264	9830	0.9867	1.012	198.90176	54.725
10	42177	10297	39428	9626	42078	10273	0.9348	1.067	197.14048	109.8729
20	42455	10365	38838	9482	42361	10342	0.9148	1.091	194.19136	141.094
30	42746	10436	37966	9269	42709	10427	0.8882	1.125	189.82912	169.624
40	43008	10500	37929	9260	42918	10478	0.8819	1.132	189.6448	192.752
50	43467	10612	37552	9168	43266	10563	0.8639	1.152	187.76064	257.737

TABLE 5.3

PERFORMANCE EVALUATED FOR PROTOCOL AODV WITH SMT

No of Malicious Nodes	AGT - SENT		AGT - RECEIVED		RTR - SENT		PDR	ROUTING LOAD	THROUGHPUT (kb/s)	End-to-End Delay (ms)
	Kb	PACKETS	Kb	PACKETS	Kb	PACKETS				
0	40317	9843	39780	9712	40264	9830	0.9867	1.012	198.90176	54.725
10	40227	9821	39584	9664	40174	9808	0.9840	1.015	197.91872	70.74
20	40223	9820	39543	9654	40468	9880	0.9831	1.023	197.71392	86.266
30	41722	10186	39552	9888	41652	10169	0.9707	1.028	197.76	101.178
40	41791	10203	39470	9712	41722	10186	0.9519	1.049	197.34784	143.53
50	41947	10241	39285	9591	42287	10324	0.9365	1.076	196.42368	148.305

5.7 Summary

OTCL script is added to the TCL script in the normal AODV protocol for added features that allow finding the multipath load balancing and message dispersion. The results are obtained in adverse conditions where half of the nodes in the network are malicious. The results are visualized in the nam simulator and the four characteristics: end-to-end delay, packet delivery ratio, throughput, and routing load are tested. It is observed that in adverse conditions, the AODV protocol with SMT protocol gives better performance results than normal AODV protocol.

CHAPTER 6

CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

This thesis aimed to compare the normal AODV protocol with the combined AODV protocol and the SMT protocol. The NS-2 simulator was used for the simulations. The simulation scenario with packet drops due to malicious nodes or high traffic was generated and the simulation time is fixed with varying malicious nodes of 0, 10, 20, 30, 40 and 50 at pause time of 2 ms. Other parameters were kept constant. The following observations were recorded. Initially in the case of the AODV protocol, there was considerably low packet loss, which increased with an increase in the number of malicious nodes. In the case of the AODV protocol with the SMT protocol, simulation showed that the packet loss was very low initially and it is maintained constantly throughout the simulation period, although the number of packet drops increased.

Hence, the AODV protocol should be preferred when the MANET has to be configured for a fewer number of adversaries (malicious nodes) due to the low initial packet loss as observed in the AODV protocol. Whereas, in the presence of a lot of adversaries, the AODV protocol with the SMT protocol should be preferred since the packet loss was less. In comparison with the normal AODV protocol, the AODV protocol in combination with the SMT protocol has better packet delivery ratio. In the presence of malicious nodes, the AODV protocol with the SMT protocol performed better in terms of all four performance measures: end-to-end delay, packet delivery ratio, throughput, and routing load.

6.2 Future Work

In this thesis, a number of parameters were kept constant. Future work might involve varying these parameters in the two protocols and observing the network behavior. An open

issue of interest is how to obtain estimates or predictions of the probability that a route will be operational. The complexity of such a task is increased because of the numerous factors that affect the condition of the utilized routes. Mobility, congestion, transmission impairments, and an arbitrary, possibly intermittent, changing-over-time attack pattern, must be taken into consideration. Through interaction with the network and feedback obtained from the trusted destination, each node can gradually "construct" such estimates. Clearly, the network conditions and characteristics can change over time. More simply, parameters such as network connectivity, density, or number of attackers present can differ according to the nodes' neighborhood. In any case, a feasible estimation method would be able only to continuously track such changes and provide rough estimates. Finally, despite the use of re-transmissions, the AODV protocol with the SMT protocol does not assume the role of a transport layer protocol - it operates at the network layer to secure data forwarding and to significantly improve the reliability of message delivery. However, this protocol provides security and protects from frequent disruptions at the expense of increased traffic in the network, especially when data loss is detected.

REFERENCES

REFERENCES

[1] G. Lin, G. Noubir and R. Rajmohan "Mobility models for ad hoc network simulation," in *Proceedings of INFOCOM Twenty-Third Annual Joint Conference of the IEEE Computer and Communications Societies*, - November 2004.

[2] "Mobile Ad-Hoc Networks (MANET)," http: //www.ietf.org/rfc/rfc2501.txt., January 1999.

[3] I. D. Chakeres and E. M. Belding, "AODV routing protocol implementation design," in *Proceedings of the international workshop on wireless ad hoc networking, Tokyo, Japan,* March 2004

[4] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference,* January 2002.

[5] J. Broch, David A. Maltz, David B. Johnson, Y-Ch Hu, and J Jetcheva, "A performance comparison of multi-hop wireless ad hoc network for mobile ad hoc networks", in *Proceedings of 4th annual IEEE/ACM international conference on Mobile Computing and Networking,* pp. 85-97, October 1998.

[6] Z. Ismail and R. Hassan, " Performance of AODV routing protocol in mobile ad hoc networks," in *Proceeding of Information Technology (ITSim), 2010 International Symposium*, pp. 1 – 5, 15-17, June 2010.

[7] Department of Computer Science, Uppasala University, AODV-UU. http://core.it.uu.se/core/index.php/AODV-UU, [Retrieved on July 2010].

[8] Gupta, Prinima and R. K. Tuteja, "Design strategies for AODV implementation in Linux," in *International Journal of Advanced Computer Science and Applications,* Vol. 1 No. 6, December 2010.

[9] T. Buchheim, "NS-2 - The Network Simulator – ns-2 homepage", in http://www.isi.edu.nsnam/ns/ July 2001, [Retrieved on Aug 2009].

[10] E. M. Royer, P. M. Melliar-Smith, and L. E. Moser. "An Analysis of the Optimum Node Density for Ad hoc Mobile Networks," in *Proceedings of the IEEE International Conference on Communications (ICC) 2001*: 15 June 2011.

[11] Jean Tourrilhes, "3.1 Lucent Wavelan IEEE, Lucent Orinoco, Enterasys Roam About 802, Elsa AirLancer 11 and Melco/Buffalo 802.11b." *The devices, the drivers - 802.11b*. July 2007.

[12] P. Papadimitrattos and Z. J. Haas, "Secure message transmission in mobile ad hoc networks," *Elsevier Ad Hoc Networks Journal,* Vol. 1, no. 1, March 2003.

APPENDICES

APPENDIX A

TCL SCRIPT USED FOR SIMULATIONS

```
#
=====================================================================
=
# Define options
#
=====================================================================
=
set val(chan)       Channel/WirelessChannel
set val(prop)       Propagation/TwoRayGround
set val(netif)      Phy/WirelessPhy
set val(mac)        Mac/802_11
set val(ifq)        Queue/DropTail/PriQueue
set val(ll)         LL
set val(ant)        Antenna/OmniAntenna
set val(x)            520   ;# X dimension of the topography
set val(y)            520   ;# Y dimension of the topography
set val(ifqlen)         100           ;# max packet in ifq
set val(seed)         0.0
set val(adhocRouting)   AODV
set val(nn)           100           ;# how many nodes are simulated
```

```
set val(cp)             "../mobility/scene/cbr-3-test"
set val(sc)             "../mobility/scene/scen-3-test"
set val(stop)           200.0           ;# simulation time
#
# ======================================================================
# Main Program
# ======================================================================
#
# Initialize Global Variables
#
set ns_             [new Simulator]
set tracefd     [open aodvlatest.tr w]
$ns_ trace-all $tracefd


set namtrace [open aodvlatest.nam w]          ;# for nam tracing
$ns_ namtrace-all-wireless $namtrace $val(x) $val(y)
# set up topography object
set topo       [new Topography]
$topo load_flatgrid 520 520
#
# Create God
```

```
#
create-god $val(nn)
#
# Create the specified number of mobilenodes [$val(nn)] and "attach" them to the channel.
# configure node
$ns_ node-config -adhocRouting $val(adhocRouting) \
                 -llType $val(ll) \
                 -macType $val(mac) \
                 -ifqType $val(ifq) \
                 -ifqLen $val(ifqlen) \
                 -antType $val(ant) \
                 -propType $val(prop) \
                 -phyType $val(netif) \
                 -channelType $val(chan) \
                 -topoInstance $topo \
                 -agentTrace ON \
                 -routerTrace ON \
                 -macTrace OFF \
                 -movementTrace OFF

        for {set i 0} {$i < $val(nn) } {incr i} {
                set node_($i) [$ns_ node]
```

```
                $node_($i) random-motion 0              ;# disable random motion
        }
# Command used to set random location for the nodes
# setdest -v 1 -n 100 -p 2 -M 20 -t 200 -x 520 -y 520
# nodes: 100, pause: 2.00, max speed: 20.00, max x: 520.00, max y: 520.00
#
set god_ [God instance]
$node_(0) set X_ 407.242847654622
$node_(0) set Y_ 356.599838862374
$node_(0) set Z_ 0.000000000000
$node_(1) set X_ 278.537839403346
$node_(1) set Y_ 269.676025163525
$node_(1) set Z_ 0.000000000000
# Similarly, the configuration (program lines) are executed for nodes 2 to 99
# Command used for UDP connections between nodes
# ns cbrgen.tcl -type cbr -nn 100 -seed 1.0 -mc 38 -rate 4.0
# The rate can be varied according to the maximum number of paths required. A rate of 4 is
#sufficient to obtain the optimal control overhead for 38 nodes. This rate value is chosen for
#AODV with SMT but not for normal AODV
# nodes: 100, max conn: 100, send rate: 0.25, seed: 1.0
#
for {set i 0} {$i < $val(nn)} {incr i} {
```

```
 # 20 defines the node size in nam, must adjust it according to your scenario
# The function must be called after mobility model is defined
$ns_ initial_node_pos $node_($i) 2
}
for {set i 0} {$i >20}{$i<30} {incr i} {

# no of malicious nodes is 10 and we vary the node size for every simulation, these malicious
#nodes drop all the incoming and outgoing packets for no reason
ErrorModel set rate_ 0.1
proc UniformErrorProc {} {
    global opt
   set errObj [new ErrorModel]
    $errObj unit packet
    return $errObj
}
#
# Tell nodes when the simulation ends
#
for {set i 0} {$i < $val(nn) } {incr i} {
    $ns_ at 150.0 "$node_($i) reset";
}
$ns_ at 150.0 "stop"
```

```
$ns_ at 150.01 "puts \"NS EXITING...\" ; $ns_ halt"

proc stop {} {
    global ns_ tracefd namtrace
    $ns_ flush-trace
    close $tracefd
    close $namtrace
}

puts "Starting Simulation..."
$ns_ run
```

APPENDIX B

AWK CODE USED TO CALCULATE END-TO-END DELAY

```
BEGIN { highest_packetid = 0; totdur=0; received = 0; start = 0; end = 0; };
{
act = $1;
time = $2;
packetid = $6;

if (packetid > high_packetid)
 high_packetid = packetid;

if(start_time[packetid]==0) {
start_time[packetid] = time;
}
if (act!= "D") {
if (act == "r") {
end_time[packetid]=time;
}
}
else {
end_time[packetid] = -1;
```

```
}
if ( act == "r" ){ received++; }
}
END {
for (packetid = 0;packetid <= high_packetid; packetid++) {
start = start_time[packetid];
end = end_time[packetid];
packet_duration = end-start;
if(start<end) {
total = total+packet_duration;
printf("%d %f %f \n", start, packet_duration, total);
}
}
}
```