PERFORMANCE EVALUATION OF A SECURED AD-HOC ROUTING PROTOCOL

By

DHEERAJ BABU GULLURU

Bachelor of Technology in Computer Science

Jawaharlal Nehru Technological University

Hyderabad, Andhra Pradesh

2002

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
May, 2006

PERFORMANCE EVALUATION OF A SECURED

AD-HOC ROUTING PROTOCOL

Thesis Approved:

Dr. JOHNSON P THOMAS
Thesis Adviser

Dr. NOHPILL PARK

Dr. VENKATESH SARANGAN

A. GORDON EMSLIE
Dean of the Graduate College

ACKNOWLEDGEMENTS

My sincere thanks are due to my adviser Dr. Johnson Thomas, without his motivation, encouragement and support this thesis effort would not have been possible. I am greatly indebted for his guidance both on personal and professional fronts.

I would also like to thank my committee members Drs. Nohpill Park and Venkatesh Sarangan for serving on my committee. Their guidance and suggestions are greatly appreciated.

I am greatly indebted to Dr. J Paul Devlin for supporting me on professional and financial fronts.

I would like to thank my mother Mrs. Koteswari and my father Mr. Haranath Babu and my sisters Miss. Mrudula and Neelima for their love and support throughout the years.

Finally I would like to thank Sravani, Mahesh, Vamsi and all my friends who stood beside me with their unfailing and indispensable support.

TABLE OF CONTENTS

LIST OF FIGURES

Figure Page

CHAPTER I

INTRODUCTION

Wireless technology allows users to access information and services electronically irrespective of geographical position. Wireless technology has become tremendously popular due to its usage in various new fields of applications in the domain of networking. One such important field is Mobile Ad-hoc Networks (MANET's) where the nodes of the network do not have a specific infrastructure and they are connected dynamically in an arbitrary manner. Nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. Nodes in an ad-hoc network move dynamically; consequently keeping track of the network topology is a difficult task to achieve. There are many security issues associated with these kinds of networks. Security in wired networks can be applied to some extent but ad-hoc networks have their own vulnerabilities which cannot be always plugged using wired security issues. Although security has been achieved to some extent, attacks keep increasing in the form of malicious nodes which may jam or spoof the channel or drop the packets.

Many routing protocols have been proposed for Ad hoc networks. Recently secure routing protocols have also been proposed [Zapata 02, Deng et al. 02]. If the introduction of secure mechanisms into routing degrades the performance significantly, the network designer has to evaluate the trade-offs in introducing security into routing. However, to

the best of our knowledge no one has investigated the overheads associated with introducing security into routing protocols. This thesis concentrates on one such routing protocol namely Ad hoc On Demand Vector Routing Protocol (AODV) [Perkins and Royer 99]. We compare AODV with secure AODV [Perkins and Royer 99] and study the impact of security on routing overhead and on other performance metrics.

Thesis Outline

In chapter 2, a brief introduction to ad hoc networks is given along with their applications and characteristics. The AODV and the secure AODV routing protocols are discussed as a part of the literature review in chapter 3. Research objectives, scope and research methodology are described in chapter 4. The simulation model, implementation details and results are presented in chapter 5. Chapter 6 concludes the thesis and provides suggestions for future research.

CHAPTER II

AD-HOC NETWORKS

An ad-hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure [Perkins and Royer 99]. The primary goal of ad-hoc networks is to set up communications for specialized, customized applications in areas where there is no infrastructure (e.g., battlefield, jungle operations), or where the infrastructure has failed (e.g., earthquake rescue) and most of the ad hoc applications are mobile. Typically ad hoc networks are set up for a limited amount of time. The protocols are tuned for the particular application (e.g., send a video stream across battlefield; find out if a fire has started in the forest etc.). The application may be mobile and the environment may change dynamically (figure 2.1.) and nodes communicate via wireless signals. Routing protocols help the nodes to communicate in order to accomplish the task.

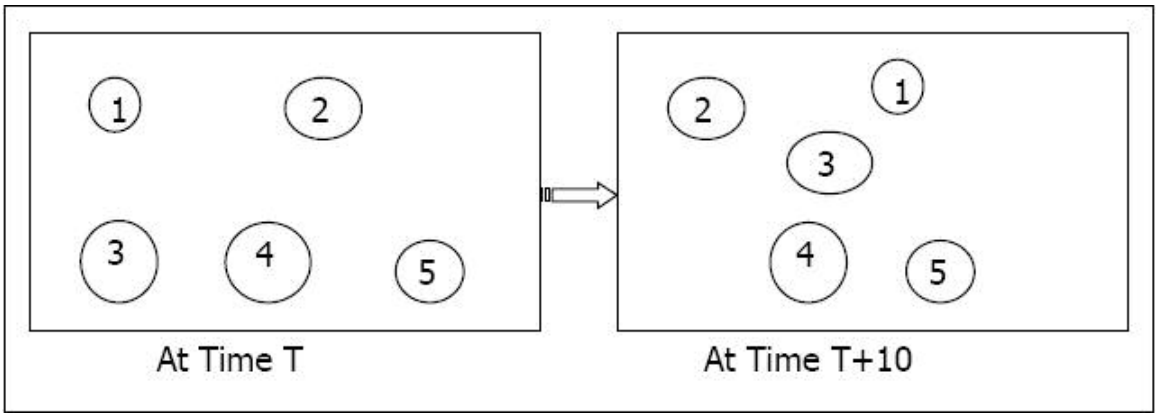

Figure 2.1. Ad-hoc network dynamic topology

2.1. Characteristics of Ad-hoc networks

Mobility: Ad hoc nodes are mobile in nature; they dynamically move in a network in order to achieve a specific task. Rapid deployment in areas with no infrastructure often implies that the users must explore an area or form teams that in turn coordinate among themselves to create a task force or mission. The mobility model can have serious impact on routing which in turn may affect the performance of the network.

Multihopping: A multihop network is a network where the path from source to destination traverses several other nodes. Ad-hoc networks may exhibit multiple hops for obstacle negotiation and energy consumption.

Energy Conservation: Mobile nodes in an ad hoc network may depend on batteries or other kinds of energy sources for their energy. Minimizing energy consumption in an ad-

hoc network is one of the biggest challenges. Nodes which form a dominating set in a network are chosen and energy consumption of nodes with in the particular set is optimized.

Security: Security is considered to be the primary concern in an ad hoc network. Providing a secured communication channel for nodes and keeping track of malicious or compromised nodes are major concerns in ad-hoc networks.

Scalability: In an ad-hoc network scalability can be handled using hierarchical construction. If mobility is limited then scalability can be easily handled using mobile IP and local handoff techniques. Some networks have a large number of nodes, and the techniques which are applicable for limited mobility do not work well in such cases. High mobility is one of the biggest challenges in ad-hoc design.

Routing Protocols: Routing protocols in an ad-hoc network are meant for communication between nodes. Node mobility is highly dynamic in ad hoc networks causing frequent route failures. A good routing protocol should adapt to a dynamic topology and it should be energy and bandwidth efficient. Routing protocols are primarily classified into Table driven and On demand routing protocols.

2.2. Applications

Ad-hoc networks do not require any infrastructural setup and there is no delay in setting up the network Data exchange takes a very minimal time. This feature makes ad-hoc network suitable to situations such as battle field, rescue, jungle operations etc.,

where there will be no fixed infrastructure. Figure 2.2 shows how an ad-hoc network is applicable to the above mentioned situations.

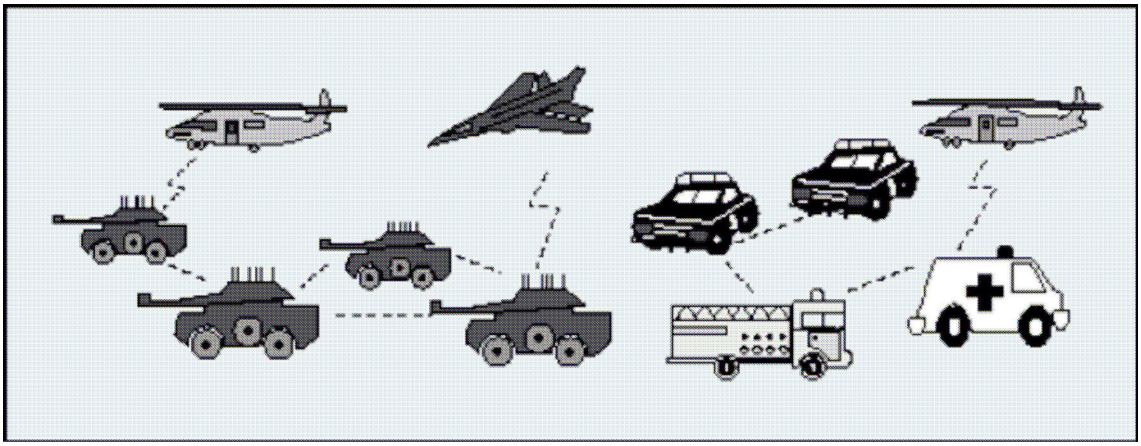

Figure 2.2. Example applications of MANET [from Deng et al. 02]

Ad-hoc Networks are developed to setup communications for specialized applications and they also provide instant connectivity across different communication devices irrespective of their location and underlying technology. The applications are mobile and they are required in situations where the infrastructure has failed. This is considered to be an important goal in networking and is shown for a military situation in figure 2.3.

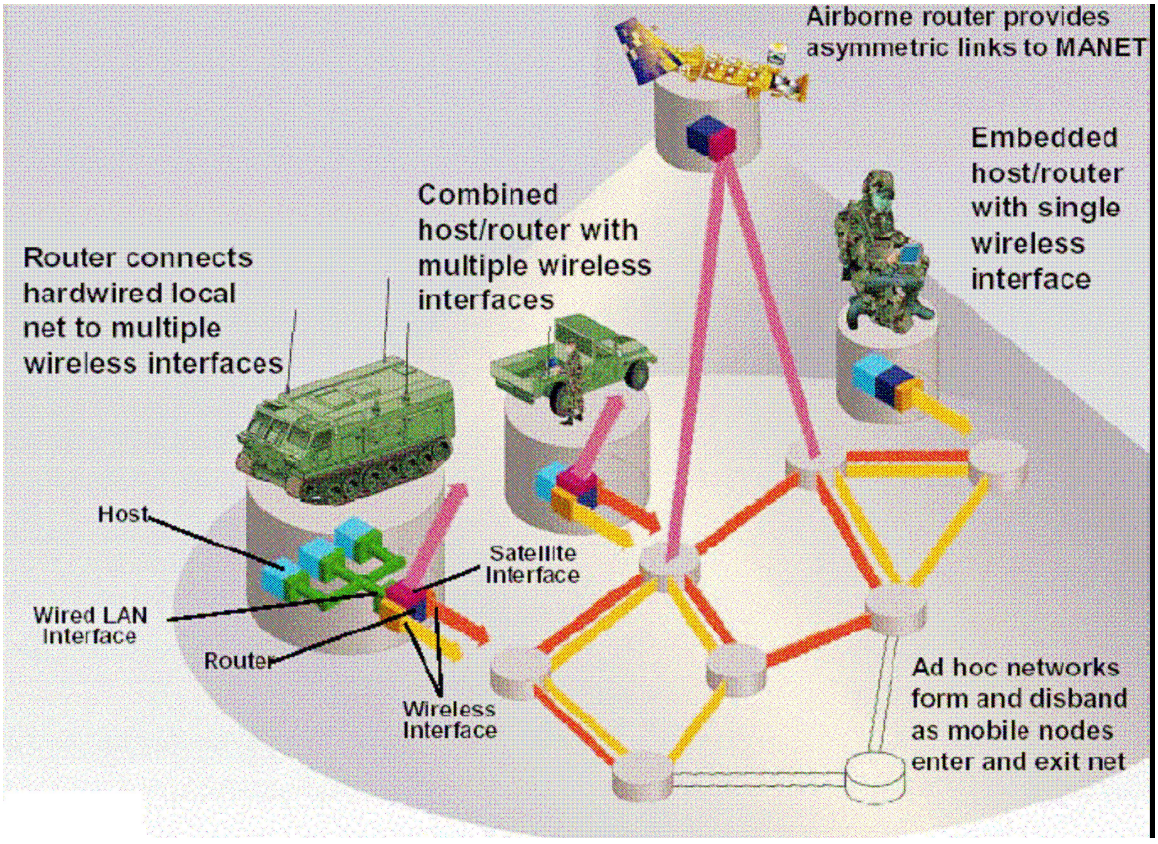

Figure 2.3. A typical ad-hoc network in a military situation [from Corson 02]

CHAPTER III

LITERATURE REVIEW

In this chapter the Ad-hoc on Demand Distance Vector Routing (AODV) and secure AODV routing protocols are described in detail.

3.1. Ad-hoc on Demand Distance Vector Routing (AODV) [Perkins and Royer 99]

AODV is an on demand distance vector routing algorithm. In AODV each mobile host acts as a specialized router and routes are obtained as needed (i.e., on demand). Routes are maintained only between the nodes which need to communicate. It is suitable for dynamic self starting networks. It also provides loop free routes and even repairs broken links by notifying the nodes so that they can invalidate the route using the lost link. The overall bandwidth required for this protocol is smaller compared to other protocols since it doesn't require any global periodic advertisements

Primary Objectives

AODV allows mobile nodes to obtain routes quickly for new destinations and it also allows mobile nodes to respond to changes in the network topology and link breakages in a timely manner. Nodes that are not in active communications neither participate in the routing exchanges nor maintain any routing information. Neighborhood detection can be

performed using local broadcasts such as "*hello messages*".

- Discovery packets are broadcasted by the source node when a necessity for a new route occurs.
- Local connectivity management and general topology maintenance should be properly distinguished.
- Changes in local connectivity management should be intimated to the neighboring nodes in a proper way.

Path discovery

Path discovery is initiated when a source node communicates with another node for which it has no routing information in its table. Each node maintains two counters, node sequence number and broadcast ID. Path discovery is initiated by broadcasting route request (RREQ) packets to its neighbors. The source broadcasts the route request packets to its neighbors. The neighbors in turn sends the packets to their neighbors until the packet reaches an intermediate node which has recent route information for the destination or it till reaches the destination itself. Nodes discard the packets which they had already seen. The RREQ packet contains the following fields:

<*source_addr, source_sequence#, broadcast_id, dest_addr, dest_sequence#, hop_count*>

The pair < *source_addr, broadcast_id* > uniquely identifies a RREQ packet.

RREP packet contains the following fields:

<*source_addr, dest_addr, dest_sequence#, hop_count, lifetime*>

Each node either satisfies the RREQ packet by sending a route reply (RREP) back to the source (only when the RREQ packet reaches an intermediate node which has route to the destination node) or rebroadcasts the RREQ packet to its neighbors after increasing the *hop_count*.

Reverse Path Setup

The source sequence number in RREQ maintains the freshness information about the reverse route to the source whereas the destination sequence number specifies the information of the fresh route to the destination which is accepted by the source. Reverse path is automatically setup when RREQ packet travels from source to various destinations. These reverse path entries are preserved until a reply is sent back to sender.

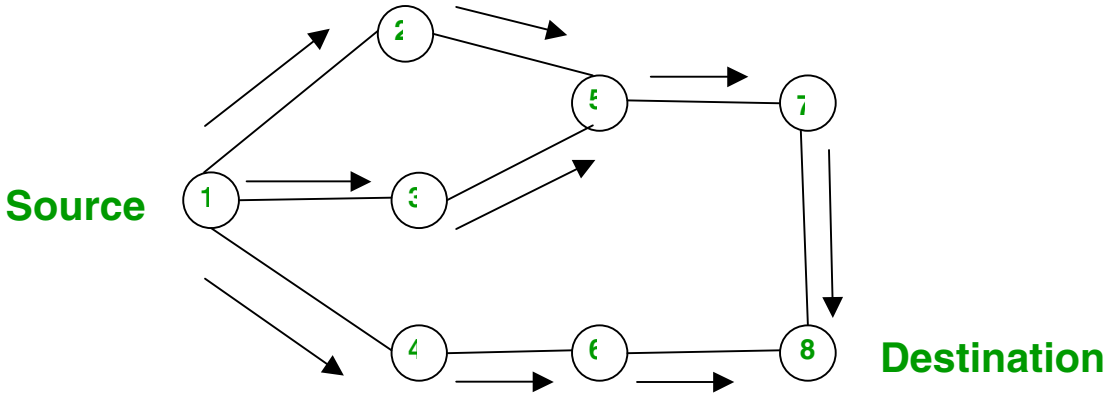

Figure 3.1. Propagation of a Route Request (RREQ) Packet

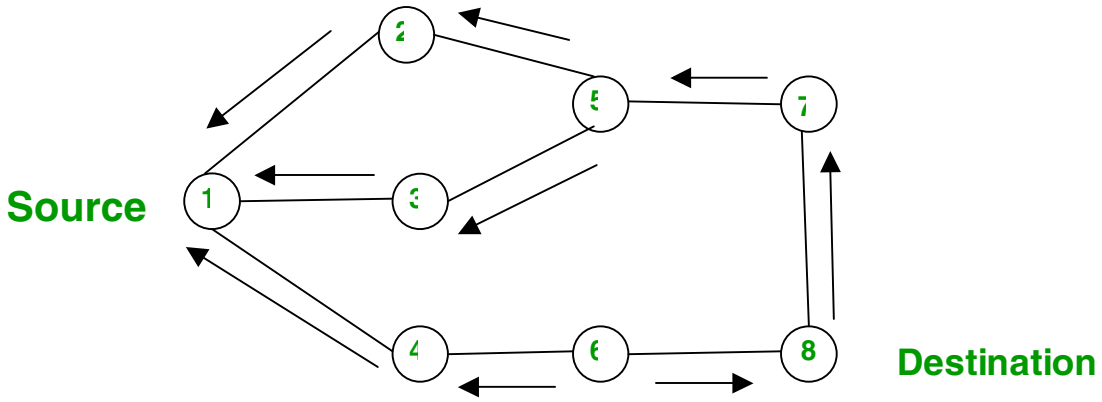

Figure 3.2. Reverse Path Formation

Forward path setup

A RREQ eventually reaches an intermediate node which has route information for the destination and the receiving node checks whether the RREQ packet has come through a bi-directional link and it compares the destination sequence number in its own route entry to that of in RREQ. If the sequence number in RREQ is greater than that of the recorded sequence number then the intermediate node should not use its recorded route information to satisfy the RREQ. The intermediate node again rebroadcasts the RREQ. The intermediate node can only respond to the RREQ if and only if the sequence number in its recorded route is greater than or equal to that of the sequence number in the RREQ. If it does not have a route to the destination or if the RREQ is not processed previously then the node unicasts a route reply packet (RREP) back to its neighbor from which it received RREQ.

The RREP travels back to the source and it sets up a forward pointer along each traversed node. Once the source node receives the RREP it begins to forward the packets to the destination. If the source receives a RREP containing a greater sequence

number or contains the same sequence number but with a smaller hop count then it will update its routing information and uses the shorter route. The RREP also updates the timeout information for route entries from source to destination and keeps track of the latest destination sequence numbers for the requested destination.

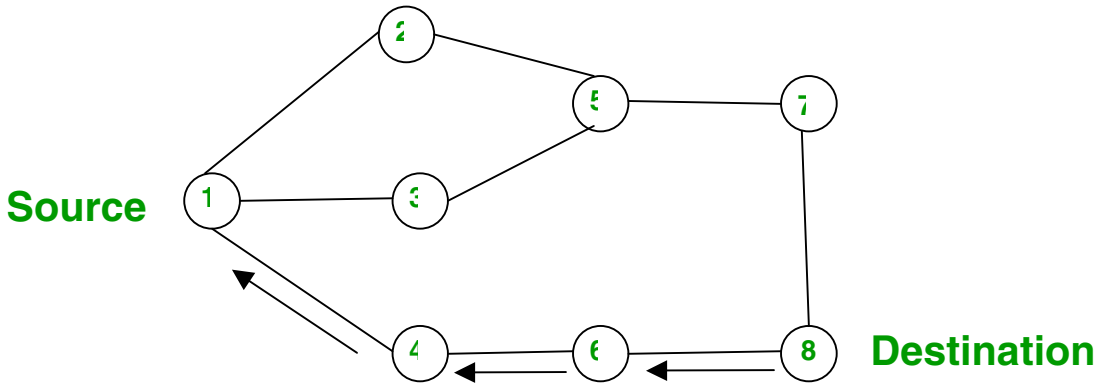

Figure 3.3. Path Taken By the Route Reply (RREP) Packet

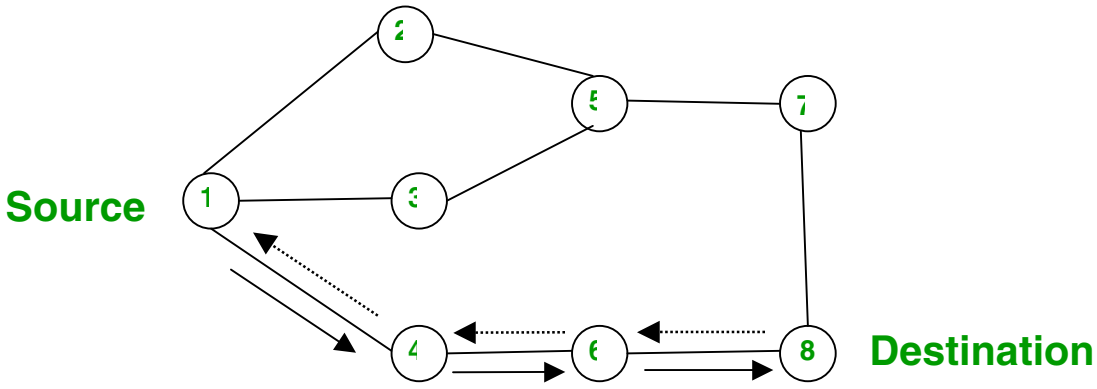

Figure 3.4. Forward Path setup

Route Table Management

Route table entries carry other useful information which is known as soft state associated with the entry. Reverse path entries contain a timer *route request expiration timer* which is used to purge reverse path routing entries from the nodes which do not lie in the path from source to destination. *Route caching timeout* is one of the most important route table entries which are used to determine when the route becomes invalid. Neighbors in a route are considered active for a destination if and only if they originate or relay at least one packet in the recent *active timeout* period. A route table contains the following information:

- Destination IP address
- Number of Hops needed to reach destination(Hop count)
- Next hop
- Destination sequence number
- Other state routing flags
- Network interface
- Lifetime of route

Whenever the source transmits data to the destination, the time limit is set to the current time plus the active route time out. If a new route is found then the source compares the destination sequence number of the new route to the destination sequence number in its routing table, if it is greater than the current one then the source assumes it to be the fresh route to destination and considers that route. If the newly offered route's destination number is same as that of the current destination number then the hop-count will be

checked, if the former one has smaller hop count then that route will be selected. Routing table will be updated if the source considers the new route with new destination sequence number and hop count.

Path Maintenance

Ad hoc nodes are mobile in nature and the nodes which are not along active path do not affect routing to a particular destination. A problem occurs when the source node moves during an active session; the source node again reinitiates the route discovery process to get the new route to destination as the previous route is invalid. If the destination node moves then it sends a special RREP packet back to the affected source nodes. Periodic *hello messages* are transmitted in order to detect link failures. Link layer acknowledgements (LLACKS) are used to detect failures. If a node fails to send a packet to the next hop neighbor then it is also a sign of link failure. When the next hop is unreachable then the node propagates a RREP packet with a new sequence number (one greater than previous known sequence number) and hop count to infinity to all the neighbors. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). When the source node gets the packet it terminates the process and starts the route discovery process again if it still needs route to destination. When the new route discovery process starts then a RREQ packet with a destination number one greater than the previous

sequence number will be broadcasted in order to ensure that the source node builds a new route to destination.

Local Connectivity Management

Nodes can know about their neighbors when they receive a broadcast from their neighbors then they will update their local connectivity information with the details of the new neighbor. A node sends a *hello message* (special RREP) which contains its identity and sequence number to the neighboring nodes and the nodes update their local connectivity information to the node. If a node receives a new broadcast or hello message from a new node or doesn't receive consecutive hello messages from its previous neighboring node then the local connectivity of the concerned node has changed.

Summary

Compared to other protocols AODV acts as an excellent choice for establishment of ad-hoc networks. Routes are obtained only when needed and nodes store only the routes which are needed. It also reduces the memory requirements and needless duplications. When a link failure occurs intermediate nodes quickly intimate the source node by broadcasting a special packet known as RERR. The source node can freshly start the path discovery process if it still needs the route to destination. Loop free routes are obtained using destination sequence numbers. AODV is suitable for large scale ad-hoc networks as the network overhead in this protocol is fairly low when compared to other protocols. However nodes in the network are assumed to be friendly; this is assumed by the authors who proposed the protocol. The later part of this document deals with

securing the AODV protocol and steps which are essential to handle malicious nodes in a network.

3.2. Secure AODV (SAODV) [Zapata 02]

The main objective of SAODV is to protect the routing information in AODV. Key management schemes are deployed in SAODV in order to securely verify the association between the address of a given ad hoc node and the public key of the node. This protocol is a pure extension to AODV by providing security features like integrity, authentication and non-repudiation. How these security features are successfully incorporated in AODV is discussed in the later part of this document.

3.2.1. *Security flaws of AODV*

A malicious node say M can carry out the following attacks in AODV.

1. Source node can be impersonated by forging RREQ with its address as originator address.
2. Change the contents of RREQ such as hop count in order to increase the chances of being in the route between source and destination. It reduces the hop count and stays in the route and analyzes the communication in the route.
3. Destination node can be impersonated by forging a RREP with its address as destination address.
4. Can act as a network leader with the biggest sequence number and sending it to the neighbors. It can become a black hole to the entire sub network.
5. It can selectively forward certain RREQs and RREPs and avoid other packets.

6. Forge a RERR message and avoids further communication between nodes as they cannot reach the destination with different sequence number.
7. Can send two different RREQs to the neighboring node with different sequence numbers which creates delay in the communication.

Security Requirements

This section discusses the requirements which are essential to secure AODV. Authorization is considered to be the prime security service. A router needs to make two types of authorization decisions. If a routing update is obtained from outside then the router needs to decide whether to update its routing information or not. This is known as *import authorization*. If a router receives request from outside for routing information then it should decide whether to send the request to other nodes, which is called as *export authorization*.

Authentication and integrity are other security services which are essential for authorization. Authentication enables a node to ensure the identity of the peer node it is communicating with. Integrity guarantees that the message sent is unaltered by any node in the network. Authentication and integrity in SAODV are achieved using digital signatures and message authentication codes. Non-repudiation is also essential in order to isolate misbehaving nodes. Non-repudiation ensures that the node which has sent the message cannot deny having sent the message. It helps in isolating the misbehaving nodes. If a router X gets an erroneous message from router Y then router X can convince other nodes that Y is malicious node by using that message. The other nodes can isolate router Y and prevent router Y from participating in the communication. The requirements in SAODV are:

- Import authorization: The route information in the route table of any node is authorized and if any malicious node lies about itself then other nodes can easily track such nodes and isolate them.
- Source authentication: Source node should be verified in order to avoid other nodes to impersonate themselves as source nodes.
- Integrity: The routing information should be verified and there should be a way to ensure that it has not been altered.
- Data authentication can be ensured by combining the source authentication and integrity services.

Data messages can however be verified using a point to point security system like IPSec. Routing messages can be altered and sent to immediate neighbors so there should be a way to secure the routing messages. A routing message carries two types of information: mutable and non-mutable. Hop count in routing message is mutable information which can be unaltered using hash chains whereas non mutable information is secured using digital signatures. These techniques are mentioned below.

SAODV Hash chains

A malicious node can alter the hop count field in the RREQ packet which is broadcasted by the source node. This increases the chances of that malicious node to stay in the route path between source and destination and thus it can analyze the communication between them. Hop count is the only mutable information present in the routing message and by using SAODV hash chains this field can be secured. Each node

(either the intermediate or destination) which receive the packet can verify that the hop count has not been decremented by the attacker. A Hash chain is formed by applying a one way hash function repeatedly to the seed.

When a node originates a RREQ or RREP message it performs the following operations:

- Generates a random number (seed).
- Sets the Max_Hop_Count field to TTL value (Time to Live) value from the IP header.

  $$Max\_Hop\_Count = TTL$$

- Sets the hash value to the seed value.

  $$Hash = seed$$

- Sets the Hash_Function field to the identifier of the hash function that it is going to use.

  $$Hash\_Function = h$$

- Calculates Top_Hash by hashing seed Max_Hop_Count times.

  $$Top\_Hash = h^{Max\_Hop\_Count}(seed)$$

  Where:

  - h is a hash function
  - $h^i(x)$ is the result of applying the function h to x i times

When a node receives a RREQ or RREP message

- Applies the hash function *h* Maximum_Hop_Count minus Hop Count times to the value in the Hash field, and verifies that the resultant value is equal to the value contained in the Top_Hash filed.

$$\text{Top\_Hash} = = h^{Max\_Hop\_Count-Hop\_Count}(Hash)$$

If it is a valid message,

- The node applies the hash function to the hash value before forwarding it.

$$Hash = h(Hash)$$

The Hash_Function field indicates which hash function has to be used to compute the hash. The Hash function should not be changed because a different hash function gives a wrong hash. Hash_Function, Max_Hop_Count, Top_Hash and Hash fields are transmitted with the AODV message, in the signature extension. All the above fields are protected using digital signatures, except the Hash field in order to protect integrity.

SAODV Digital Signatures

A digital signature is a special case of message integrity code where the code can be generated by only one participant (source). RSA signature is one kind of digital signature algorithm in which the participant only knows the private key; the participant uses the private key to produce the signature. Any other participant (node) can verify the signature using the corresponding public key. In other words a message is signed using a private key and is again verified using the public key.

Digital signatures in SAODV protect the integrity of non-mutable in RREQ and RREP messages. That means they sign everything except the hop count from AODV message and hash from SAODV extension. The intermediate nodes in AODV can reply

to a RREQ message if they have a fresh enough route to destination. Applying digital signatures to such scenarios is difficult. This particular phenomenon in AODV makes it very efficient but securing it is complicated in nature. The RREP message generated by intermediate node should sign it on behalf of the final destination. Moreover it doesn't have the signature for RREP. To overcome this problem there are two alternatives; first, if an intermediate node cannot sign the RREP message then it simply forwards the message to next node which may be the destination itself. The second alternative uses a different approach; if a node generates an RREQ message then it also includes RREP flags, the prefix size and the signature that can be used in order to reply a RREQ that asks for the node that originated the first RREQ. If an intermediate node generates a RREP message the life time of the route will be changed. So it should include both the new and old times so that the old time will be used to check the signature of the final destination. The two signature extension messages are called as RREQ and RREP double signature extensions.

When a node receives a RREQ, it verifies the signature using the public key and if the message is genuine, the message is forwarded to the next node. After verification it creates and updates reverse route to that specific host and it stores the route too. If the RREQ is received with double signature extension then the node will store the signature for RREP and the life time in the route entry. An intermediate node should reply to RREQ only if it has fresh enough route to destination or else it should simply broadcast it to the next neighbor. If the destination itself gets the RREQ then it will reply with a RREP. This RREP will be sent back with a single signature extension. When a node receives RREP then it verifies the signature and after verification it will store the route

with the signature of RREP and life time. Using digital signatures attack scenarios 1 and 3 from section 3.2.1 can be prevented.

Key Management Service

Key management service is very essential as digital signatures are employed in SAODV to protect routing information and data traffic. A public key infrastructure is employed as it is very efficient in the distribution of keys and in the achievement of integrity and non-repudiation. Efficient secret key schemes are employed in order to achieve more security and nodes authenticate each other and establish a shared session key. Each node will have a public/private key pair where the public keys are distributed to other nodes and the private keys are kept confidential by individual nodes. A trusted entity known as Certification Authority (CA) which can be used for key management holds the private/public key, with its public key known to every node and signs certificates binding public keys to nodes. The CA should stay online to reflect the current bindings, because the binding may change from time to time due to the dynamic topology of ad-hoc networks. A node should refresh its key pair as there are chances of brute-force attack on its private key. Using a single CA is very problematic in nature because if the CA is unavailable nodes cannot get the key pair. Nodes cannot have the public keys of other nodes in order to establish secure communication between them. If the CA gets compromised by revealing the private key to an adversary then the adversary can revoke the certificate and hinders the communication. A standard approach to improve availability of a service is replication. However, a naive replication of the CA makes the service more vulnerable: compromise of any single replica which possesses the service private key, could lead to collapse of the entire system. To solve this problem, trust is

distributed to a set of nodes by letting these nodes share the key management responsibility.

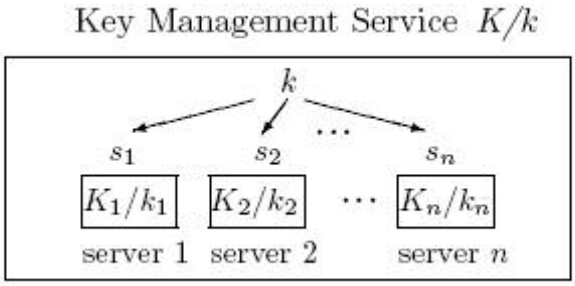

Figure 3.5. The configuration of a key management service

The key management service consists of n servers. The service, as a whole, has a public/private key pair *K/k*. The public key *K* is known to all nodes in the network, whereas the private key k is divided into n shares $s_1, s_2, \ldots, s_n$, one share for each server. Each server *i* also have a public/private key pair K_i/k_i and know the public keys of all nodes. [Hass 99]

Summary

Some of the attacks mentioned above are prevented using SAODV. Attack Scenarios 1, 3, 4 and 6 from section 3.2.1 are prevented using digital signatures. Attack number 2 from section 3.2.1 can be prevented by using hash chains. Attack number 5 from section 3.2.1 is very difficult to identify and even transmission errors can give raise to such errors. There is one attack which SAODV cannot detect that is tunneling attack. In tunneling attack two malicious nodes can simulate that they have a link between them and continuously exchange messages between them. They could achieve certain traffic

between them. These kinds of attacks can be detected using detection schemes. Hence there is a need for additional security which can prevent some attacks which cannot be identified using SAODV. Intrusion detection systems can act as a second line of defense for such attacks.

CHAPTER IV

RESEARCH STATEMENT AND METHODOLOGY

The overheads associated with secure routing protocols have not been investigated to the best of our knowledge. It is important to know the overheads and performance implications associated with secure routing so that appropriate protocols are implemented in the network. The main objective of this thesis is to find out how routing overhead and performance metrics gets affected if we provide security to a routing protocol. In this particular research AODV is chosen and a secured version of AODV (SAODV) has been implemented. These two protocols were discussed in detail and their performance evaluated.

4.1 Research Objectives

The purpose of the thesis is to develop AODV, SAODV and compare them by launching several attacks in the network. The performance of AODV and SAODV is evaluated under normal circumstances where there are no malicious nodes in the network and also under attack conditions where the network contains malicious nodes. The protocols performance is measured using the performance metrics including Packet Delivery fraction, Normalized Routing Overhead, Average end to end delay of packets and routing overhead. To achieve this, the following objectives were identified:

1) To develop and implement the AODV routing protocol.

2) To study the attacks which can be launched on AODV network such as attacks on routing messages and control messages. Attacks concerning the impersonation of nodes should also be identified.
3) To develop and implement the SAODV routing protocol which provides authentication, integrity and non-repudiation.
4) To study the impact of security on AODV routing and control messages.
5) To generate test scripts with and without attacks and test the above mentioned protocols performances on those test scripts.
6) To compare the performance of all the protocols with and without attacks in the network.
7) To suggest some measures to improvise these protocols.

4.2 Scope of the Research

The purpose of this research was to compare AODV, SAODV based on their performance under various network conditions. It also compares the protocols and how they deal with various kinds of attacks in different network scenarios. The routing protocols were simulated in ns-2 with and without attacks.

4.3 Research Methodology

In order to accomplish the objectives mentioned above, the effort is divided into the following stages

Stage 1: The existing protocols were studied and explored in detail to gain the understanding of their purpose, strengths and limitations.

Stage 2: Sample programs in ns-2 were studied and we developed some sample network scenarios based on the knowledge gained fromthe previous stage.

Stage 3: A Random way point model was developed in ns-2 to simulate the mobility of the nodes.

Stage 4: Different network scenarios such as a network with certain amount of nodes and nodes moving with different speeds were developed.

Stage 5: The AODV routing protocol was developed in ns-2 and attacks on AODV routing protocol were studied and implemented.

Stage 6: SAODV algorithm was developed in ns-2. The protocols were tested under different network scenarios.

Stage 7: Finally, the performance metrics were used to evaluate the protocols.

CHAPTER V

SIMULATION MODEL

The network simulator 'ns' is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. Node mobility, algorithm implementation and testing were done in ns-2 (Network Simulator). The speed at which a node moves in an ad-hoc network, pause time and the size of network (number of nodes) were the changing factors in the simulation runs. A detailed simulation model based on *ns-2* was used in the evaluation. The Monarch research group at Carnegie-Mellon University developed support for simulating multihop wireless networks complete with physical, data link, and medium access control (MAC) layer models on *ns-2*. The Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs was used as the MAC layer protocol. An unslotted carrier sense multiple access (CSMA) technique with collision avoidance (CSMA/CA) is used to transmit the data packets. The radio model uses characteristics similar to a commercial radio interface, Lucent's WaveLAN. WaveLAN is modeled as a shared-media radio with a nominal bit rate of 2 Mb/s and a nominal radio range of 250 m.

5.1 Traffic and Mobility Models

Traffic and mobility models employed is the same as in [Das 00] which is a common test scenario used by other performance comparison studies [Boukerche 04, Broch 98]. Continuous bit rate (CBR) traffic sources will be used. With CBR pattern, fixed size data packets were sent at roughly the same time interval and not affected by the network flow control. Thus with a CBR pattern, the performance of packet delivery is mostly determined by the performance of the routing protocols. The source-destination pairs are spread randomly over the network. The number of source-destination pairs and the packet sending rate in each pair is varied to change the traffic load in the network. For small traffic loads in networks of size 10, 20, 30, 40 nodes the packet rate is 4 packets/sec. Only 512-byte data packets are used. The mobility model uses the random waypoint model [Broch 98] in a rectangular field. The field configuration is: 1500 m x 500 m. Here, each packet starts its journey from a random location to a random destination with a randomly chosen speed (uniformly distributed between 1–20 m/s). Once the destination is reached, another random destination is targeted after a pause. The pause time, which affects the relative speeds of the mobiles, is varied. Simulations are carried out for 900 seconds. Identical mobility and traffic scenarios are used across protocols to gather fair results.

Three important performance metrics were evaluated:

Packet delivery fraction*:* The ratio of the data packets delivered to the destinations to those generated by the CBR sources.

Average end-to-end delay of data packets*:* This includes all possible delays caused by buffering during route discovery latency, queuing at the interface

queue, retransmission delays at the MAC, and propagation and transfer times.

Normalized routing load: The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.

The first two metrics are the most important for best-effort traffic. The routing load metric evaluates the efficiency of the routing protocol. These metrics are not completely independent. For example, lower packet delivery fraction means that the delay metric is evaluated with fewer samples. Path lengths play a vital role, the longer the path lengths, the higher the probability of a packet drop. Thus, with a lower delivery fraction, samples are usually biased in favor of smaller path lengths and therefore have less delay.

5.2 Simulation Implementation details:

The AODV routing protocol is already implemented in ns-2. We chose the AODV-UU protocol [UU 05] implemented by Uppsala University to incorporate security features like hash chains and digital signatures in order to realise the secured version of the AODV routing protocol. Hash chains were implemented in order to achieve the integrity of contents (to secure the mutable information) and digital signatures were used to protect the non-mutable information in RREQ and RREP packets. The intermediate node cannot send the RREP back to the node from which it received the RREQ. This is done to ensure that only single signature extensions can be used. So the destination can only send the RREP back to its previous node. This helps in fair comparison of AODV and SAODV routing protocols. The following were some of the attacks which were implemented in the simulation work.

1) Nodes which can send fake RREQ and RREP packets were created. These nodes have the different non mutable information and this information can be verified using the digital signature generated by the source node. This non mutable information can be different destination sequence number or different addresses of the source node.
2) Nodes which impersonate themselves as source and destination were also created. In these types of attacks the malicious nodes claim themselves as the source nodes and try to initiate the path discovery process by sending the fake RREQ packets to the neighbors. Since the nodes have the public key they can verify the non mutable information using the digital signature and avoid communication with them. Malicious nodes can also claim themselves as destination nodes with the highest sequence numbers. In order to prevent such attacks the sequence numbers of such nodes are assigned a very high value which is practically not possible and when the intermediate nodes try to communicate with them they will have a look at the value of the sequence numbers and simply stops communication with them. Intermediate nodes can also verify the destination node by using the digital signature.
3) Nodes which selectively forward some RREQ and RREP packets and drop the remaining packets were simulated. Simulating these kinds of attacks is a daunting task. A simple scenario is followed to handle these attacks. Every node should send at least a fixed number of hello messages to the neighboring nodes within a time frame. The neighboring nodes will keep track of the number of messages that they are receiving within the given time frame. If the number of messages are less

than the threshold then it is assumed that the attacking node is not forwarding the messages. These nodes are eliminated from the routing path.

4) A black hole situation is simulated. These nodes never forward any kind of packets which they receive and these attacks can be handled by applying the simple rule suggested above with a small change. These nodes receive the hello messages from the neighboring nodes but they won't return the reply to the neighboring nodes.
5) Nodes which can modify the routing information (mutable) were created. Hop count is the only mutable information present in the routing messages and this information can be verified using the hash chains. The hash function is applied and if it returns the wrong value then that node is considered to be a malicious node.
6) Finally the secured version of AODV is implemented so as to handle all the above mentioned attacks.

5.3 Simulation Results:

The simulation was carried out using 10, 20 and 30 nodes with the following network conditions.

- The speed is randomly chosen between 1 and 20m/s.
- The total duration for one simulation is 900s.
- The pause times were 0, 30, 60, 120, 300, 600 and 900 seconds. At 900 seconds there is no mobilitywhich means that the nodes are in a stationary condition.
- Rectangular area of 1500m x 500m was chosen and the protocols were tested using different conditions which as mentioned above.

For convenience protocols are represented in the following abbreviated forms:

- **SAODV** – Secure Ad-hoc On Demand Distance Vector Routing Protocol
- **SAODV-B** – SAODV with Bad nodes. The percentage of bad nodes were varied from 10%-50% out of the total population of nodes.
- **AODV** – Ad-hoc On Demand Distance Vector Routing Protocol
- **AODV-B** – AODV with bad nodes and the bad node population is same as that of in SAODV-B.

Each data point in the graph was an average of 5 simulations. Attack types and malicious nodes population were varied for each simulation and an average of all the results were taken into consideration.

10 NODES:

Routing overhead vs. Pause time for 10 nodes:

Routing overhead is the number of routing packets generated during the course of simulation. The below graph shows how many routing packets were generated by each protocol.

- Due to the additional security the routing overhead for SAODV, SAODV with bad nodes (SAODV-B) is obviously more compared to AODV.
- The routing overhead for AODV with bad nodes is high due to continuous route failures which occur due to the bad nodes. AODV-B therefore produces more routing packets than the normal AODV protocol.
- Routing overhead for SAODV-B is a little bit higher than SAODV due to extra routing communications needed to handle the bad nodes.

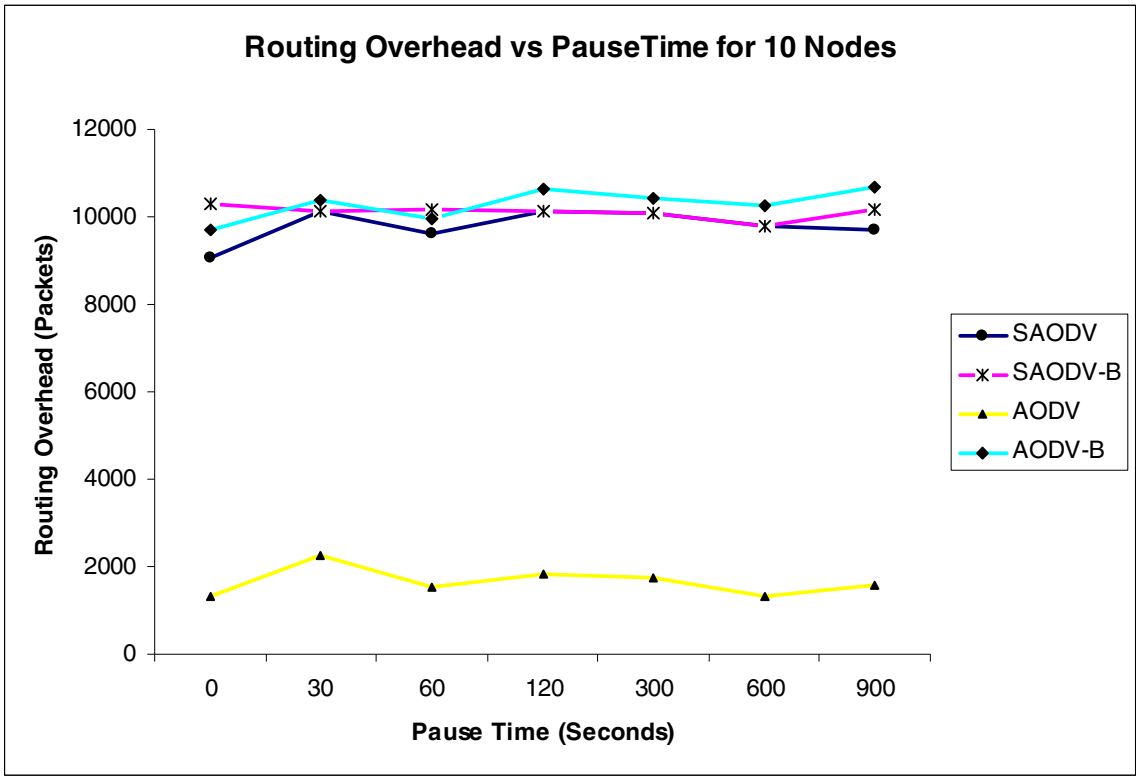

Figure 5.1. Routing overhead vs. Pause time (10 nodes).

- SAODV-B requires more routing packets since it needs to avoid the bad nodes which try to spoof the neighboring node to stay in the path by altering the mutable information present in the routing packet.

Packet Delivery Fraction vs. Pause time for 10 Nodes:

Packet delivery fraction (PDF) is the percentage ratio of number of data packets sent by the source to that of number of packets received by the destination. The below graph shows the percentage of packets generated by the source that are delivered to the destination for the four routing protocols.

- PDF is high for AODV compared to other protocols. Approximately 80% of packets were delivery from source to destination at a pause time of 0 seconds.

- With increase in the pause time the PDF decreased as the nodes have to stay at a place for more time in their journey. One reason might be the link failures which occur at these high pause times. Due to the static nature and sparseness (low density of nodes) of the network, some nodes remain disconnected from the destination for long periods of time.

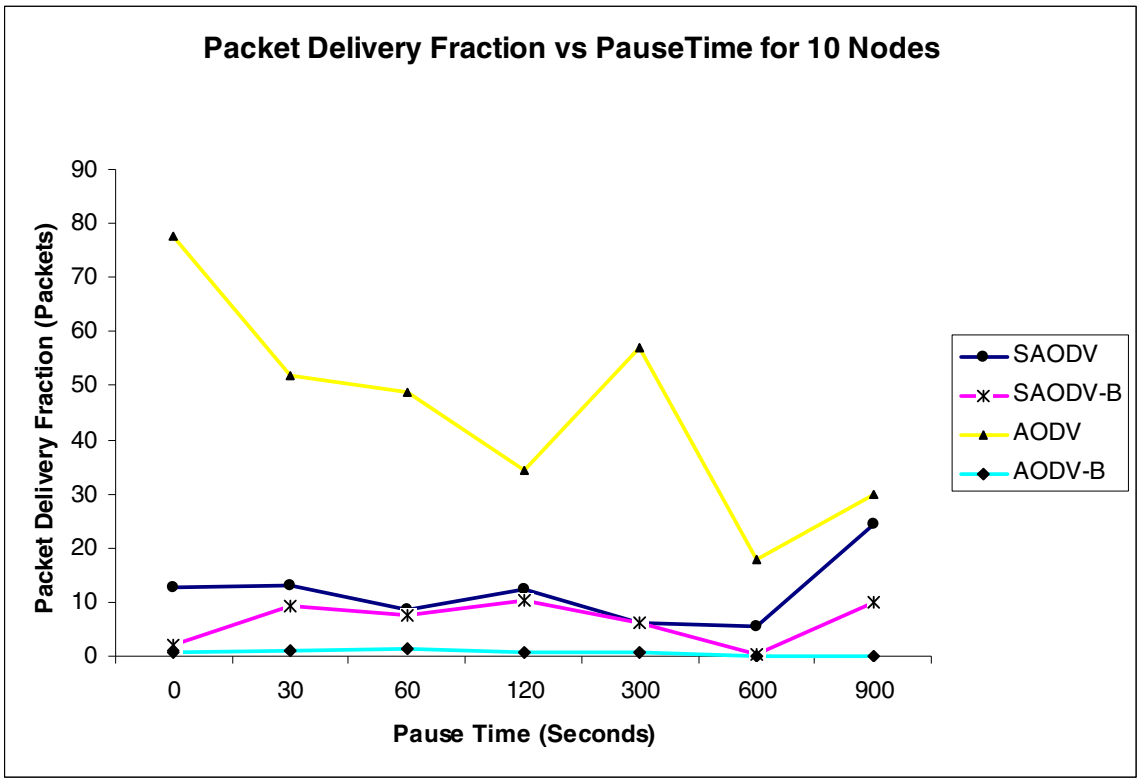

Figure 5.2. Packet Delivery Fraction vs. Pause time (10 nodes).

- For AODV-B the PDF is the least of the four protocols due to the attacks in the networks. The intermediate bad nodes may not deliver the packets which are scheduled to the destination. They simply drop the packets.
- SAODV outperformed SAODV-B in delivering the packets to the destination. SAODV-B gives a worst case performance at pause time of 600s. SAODV performed very well when there is minimal movement in the nodes.

Average End-end delay vs. Pause time for 10 Nodes

This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. The below graph shows us how this metric gets affected when the routing protocols were simulated.

- AODV-B has given worst performance due to the delays caused by the route failures, route discovery process etc.
- SAODV performed very well in this scenario compared to AODV and SAODV-B protocols.

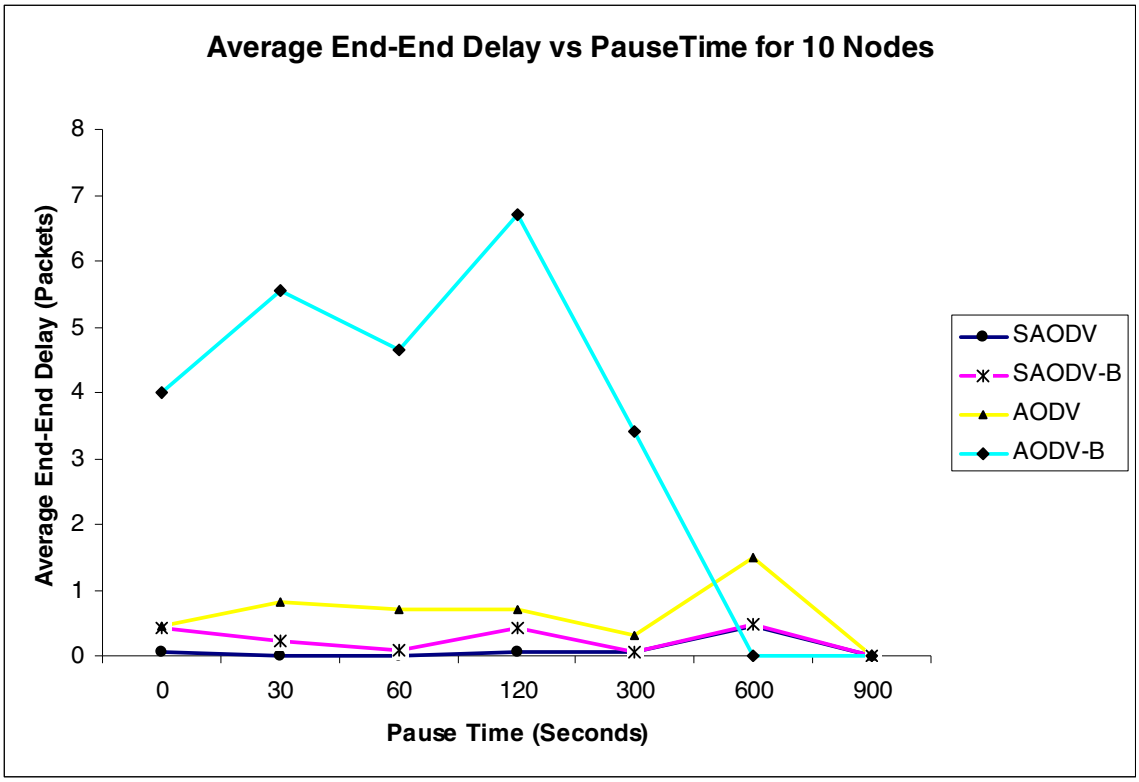

Figure 5.3. Avg. End-end delay vs. Pause time (10 nodes).

- At pause time of 900 seconds all the protocols have almost zero avg. end to end delay as there will not be any movement in nodes.
- At pause time of 120 seconds AODV-B has the highest avg. end-end delay. More delays might have occurred at that particular event of simulation due to some delays that can be attributed to the link failures and connection patterns in the network.

Normalized Routing Overhead vs. Pause time for 10 Nodes:

This is the number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.

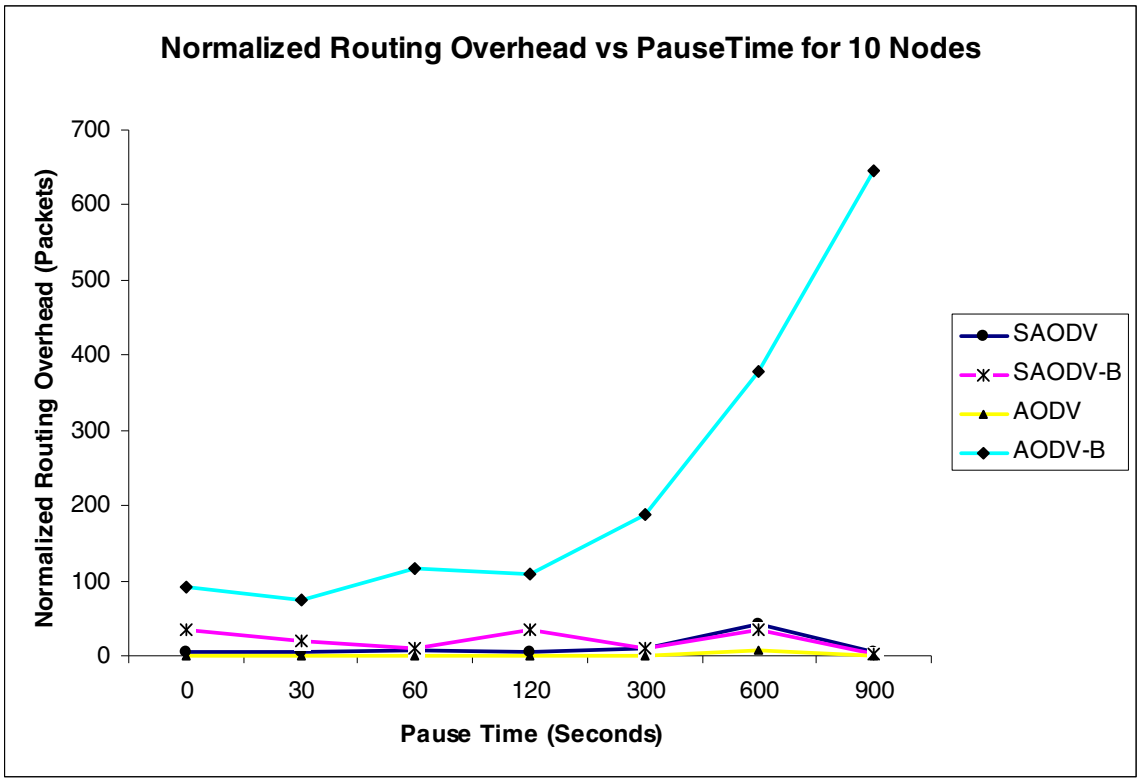

Figure 5.4. Normalized Routing Overhead vs. Pause time(10 Nodes).

- Normalized routing overhead is the number of routing packets transmitted for one data packet that reaches the destination.
- AODV outperformed all the other protocols since it consumed minimal routing packets and is clearly evident from figure 5.1.
- SAODV performed slightly better than SAODV-B in this case.
- AODV-B gives the worst performance due to the effect of bad nodes.

20 NODES:

Routing overhead vs. Pause time for 20 nodes:

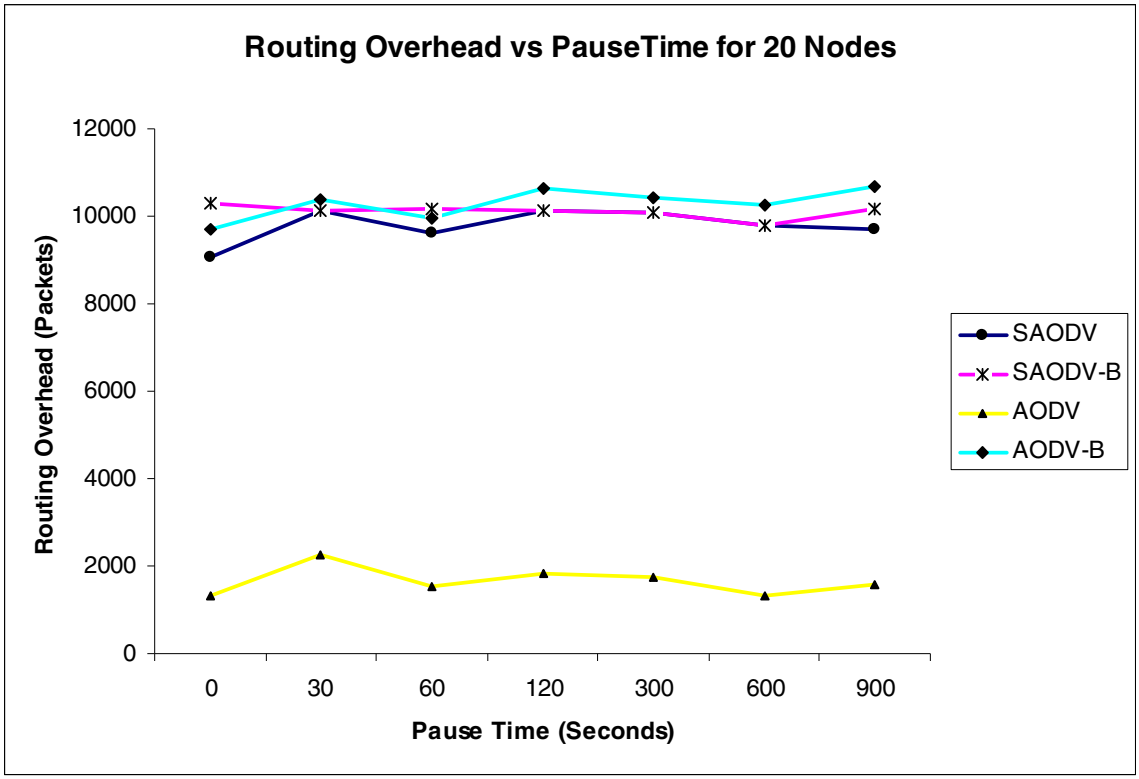

Figure 5.5. Routing overhead vs. Pause time (20 nodes).

- The number of routing packets generated by AODV-B is high compared to other

protocols, particularly at higher pause times. This can be explained due to the increase in the population of nodes/bad nodes.

- SAODV and AODV-B on an average generated same number of routing packets.
- AODV consumed minimal number of routing packets. After 60 seconds pause time the graph is almost linear.
- During the initial period of simulation SAODV-B consumed more routing packets due to continuous mobility of nodes and local connectivity changing rapidly at those high speeds.

Packet Delivery Fraction vs. Pause time for 20 Nodes:

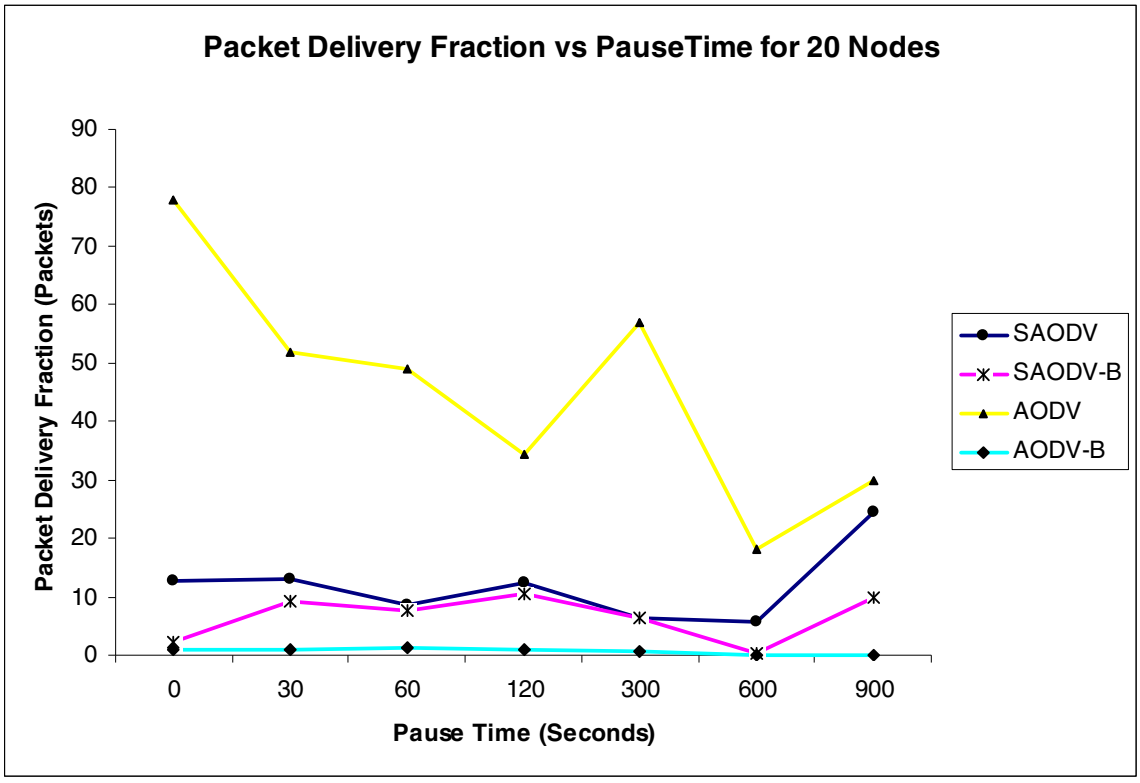

Figure 5.6. Packet Delivery Fraction vs. Pause time (20 Nodes).

- AODV outperformed the other protocols in PDF and approximately 90% of

packets were delivered for pause times 30 and 120 seconds respectively. But the performance gradually decreased thereafter and reached the lowest of 50% at 900 seconds. This may be due to the lack of mobility and sparseness of the network.

- Due to availability of more nodes and more connections between the source and destination pairs the PDF has increased compared to that of the 10 nodes network.
- SAODV performed well when compared to SAODV-B in most of the scenarios.
- AODV-B has the worst performance in this scenario. Most of the data packets were lost in their journey to the destination.

Average End-End Delay vs. Pause Time for 20 nodes:

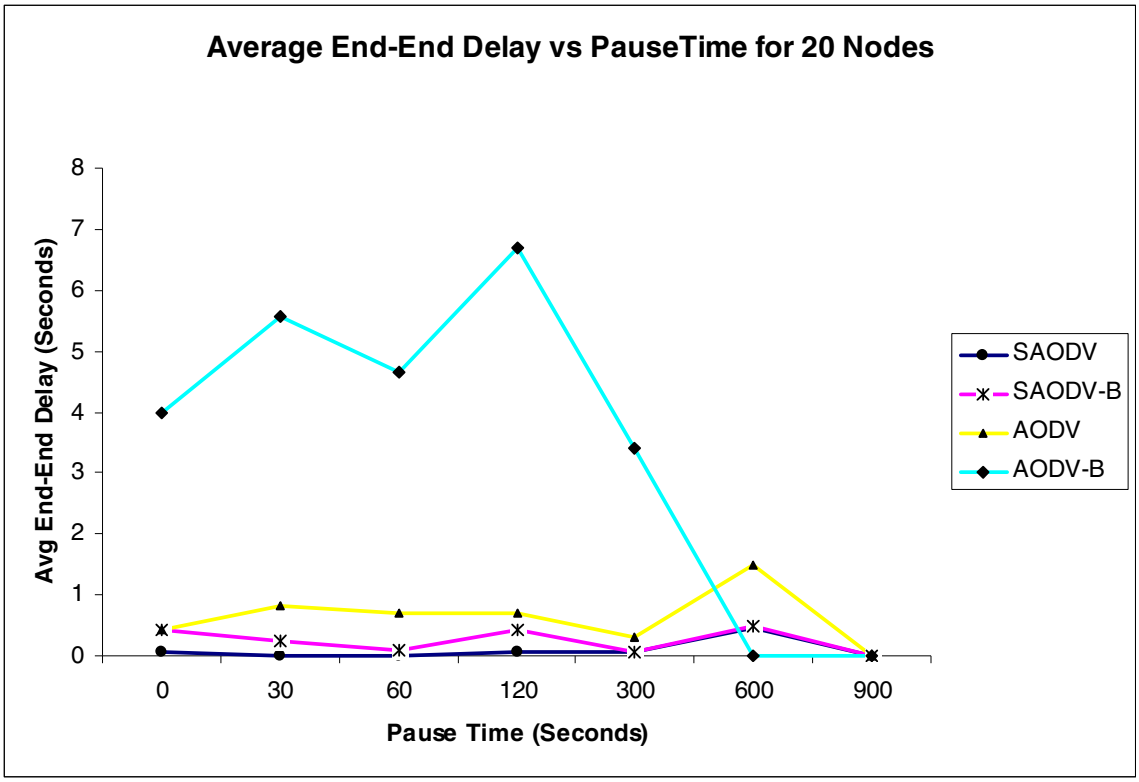

Figure 5.7. Average End-End Delay vs. Pause Time (20 nodes).

- AODV-B performance in this case is very inconsistent and the delay at pause time

0 seconds is very high and gradually decreases thereafter.

- All the other protocols have performed well in their limitations. AODV has high average end-end delay ratio at pause times 0 seconds and 30 seconds and delay is reduced in the later course of the simulation.
- The secured protocols performed well in this case.

Normalized Routing Overhead (Packets) vs. Pause time (Seconds) for 20 Nodes:

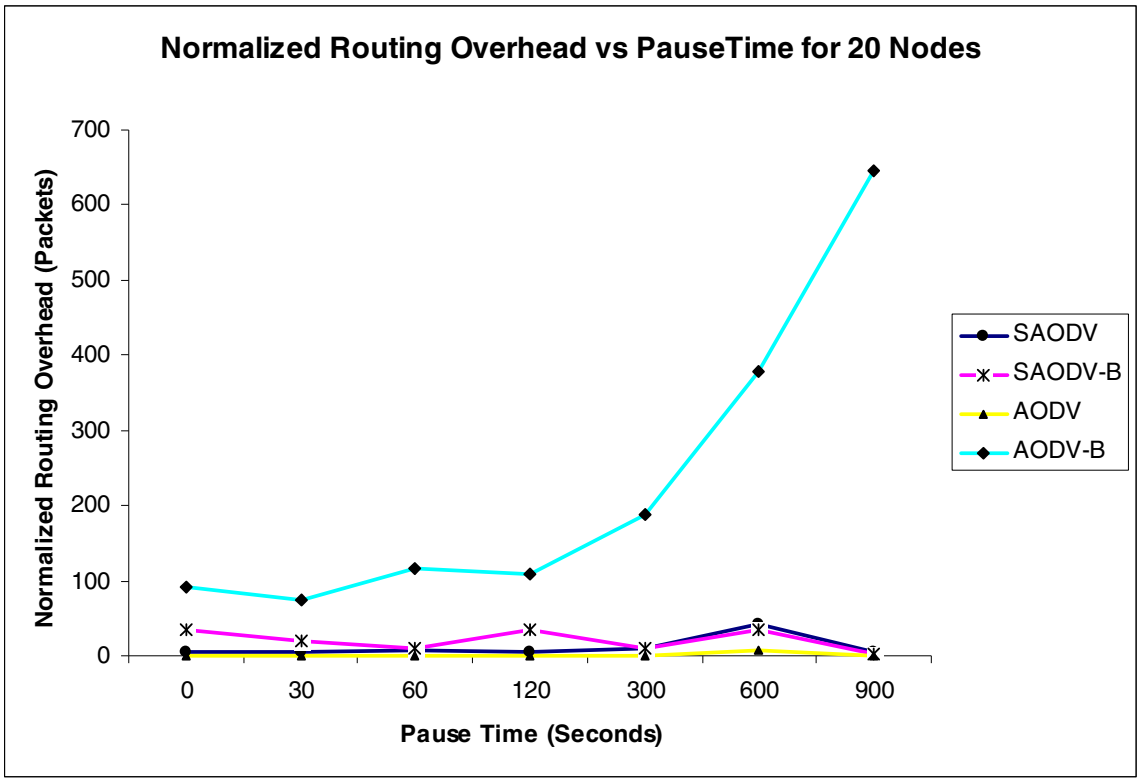

Figure 5.8. Normalized Routing Overhead vs. Pause time (20 Nodes).

- AODV-B consumes a lot of routing packets. It consumed approximately 800, 1200 routing packets for each data packet sent to the destination at pause times 60 seconds and 900 seconds.
- All the other protocols performed well and consumed minimal routing packets to

that of data packets sent.

30 NODES:

Routing Overhead vs. Pause Time for 30 Nodes:

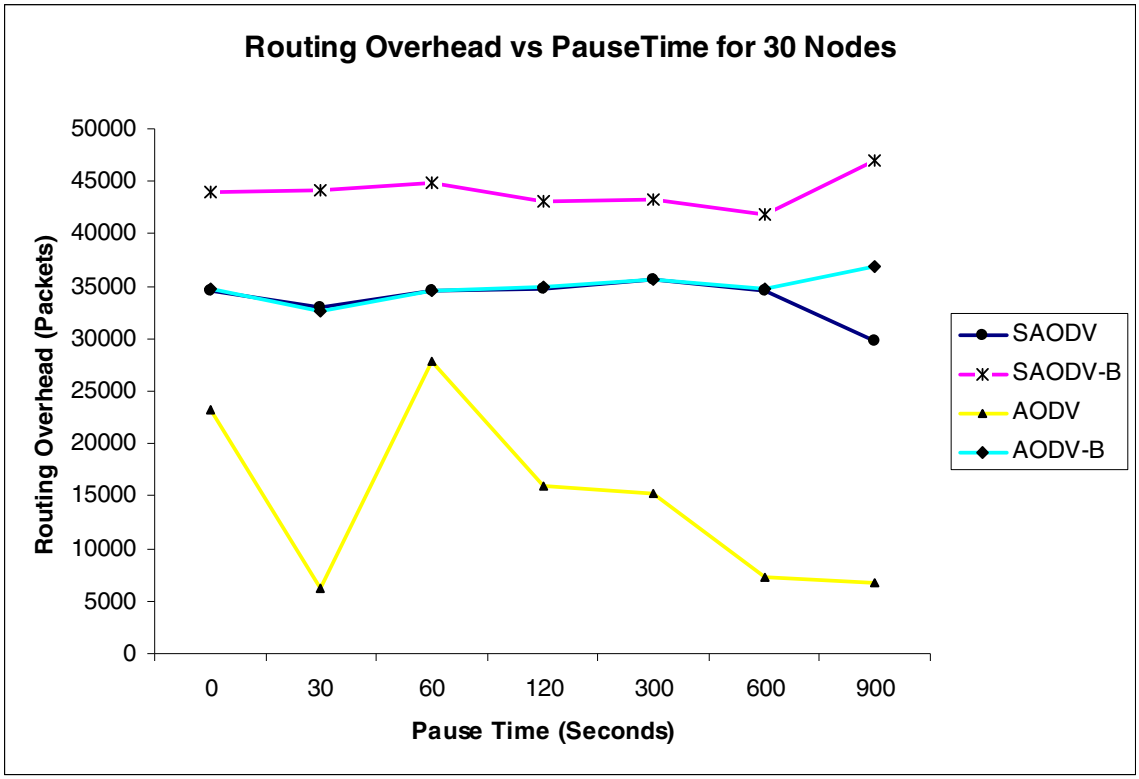

Figure 5.9: Routing Overhead vs. Pause Time (30 Nodes).

- The number of routing packets generated by SAODV-B is high compared to other protocols. This is due to the fact of malicious nodes and the protocol is tuned in such a fashion that it prevents the malicious nodes participating in active communication.
- AODV consumed the fewest number of routing packets compared to other protocols. At 60 seconds pause time it consumed more number of packets and at

pause times 30, 600, 900 seconds it consumed fewer number of packets compared to that of at 60 seconds. .

Packet Delivery Fraction vs. Pause Time for 30 Nodes:

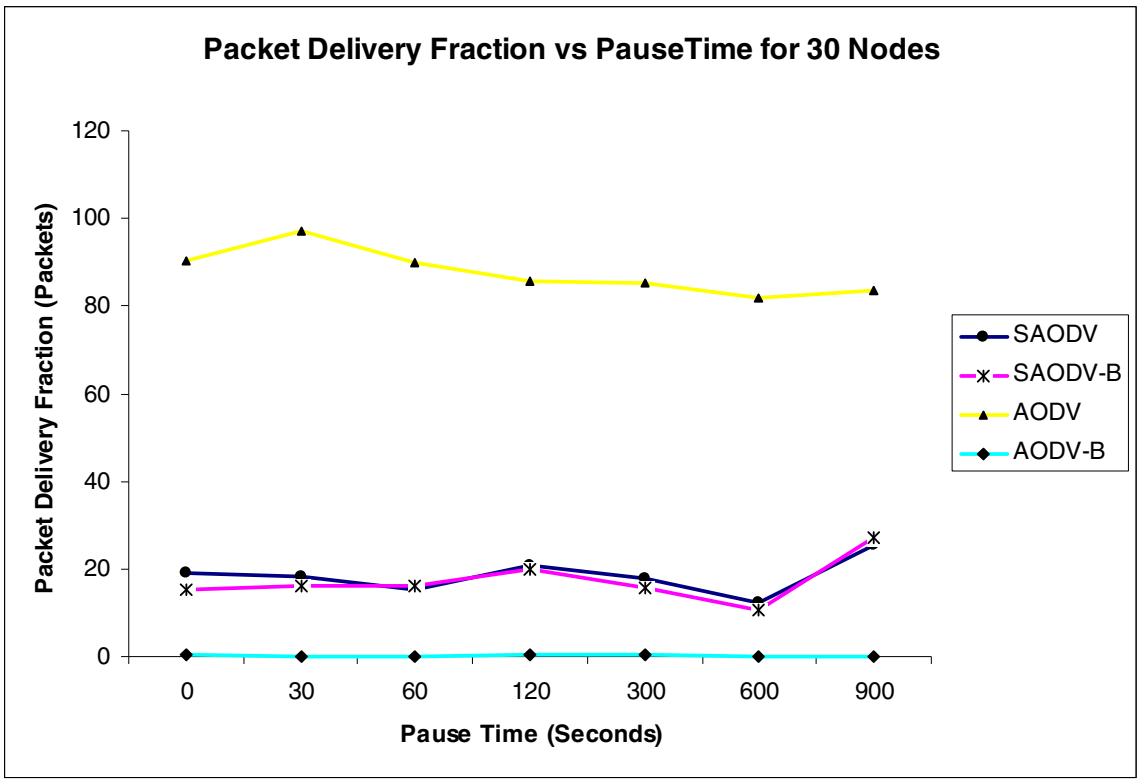

Figure 5.10: Packet Delivery Fraction vs. Pause Time (30 Nodes).

- AODV performed better compared to the other protocols. The PDF on average shows that approximately 90% of packets were delivered in all the cases. With increase in the node population, the PDF improved is evident from the above graph. Due to the availability of more nodes and more connections between the source and destination pairs the PDF has increased compared to that of a 20 node network.

- SAODV performed slightly better than SAODV-B in most of the scenarios.
- AODV-B had the worst performance in this case. Most of the data packets were lost in their journey to the destination.

Average End-End Delay vs. Pause Time for 30 Nodes:

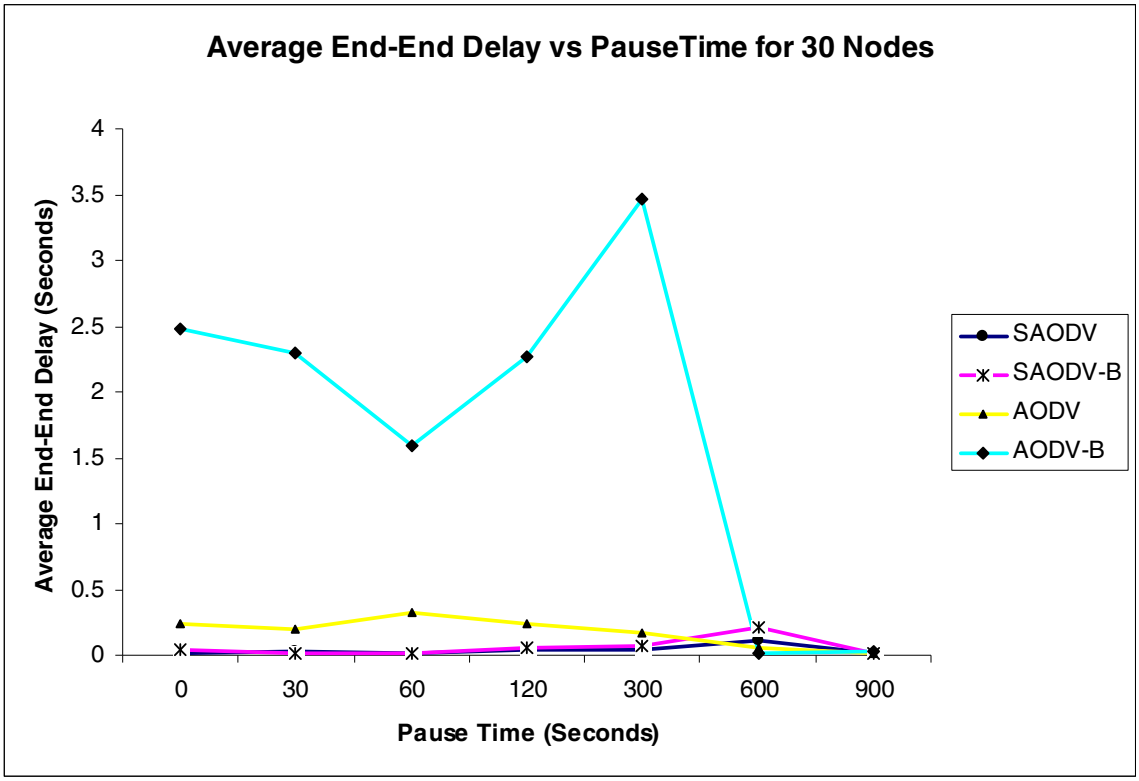

Figure 5.11: Average End-End Delay vs. Pause Time (30 Nodes).

- AODV-B routing protocol's performance has not improved and it is obviously due to bad nodes in the network which can corrupt the routing information.

Normalized Routing Overhead vs. Pause time for 30 Nodes:

- Normalizing routing overhead is still high for AODV-B even under these network conditions.

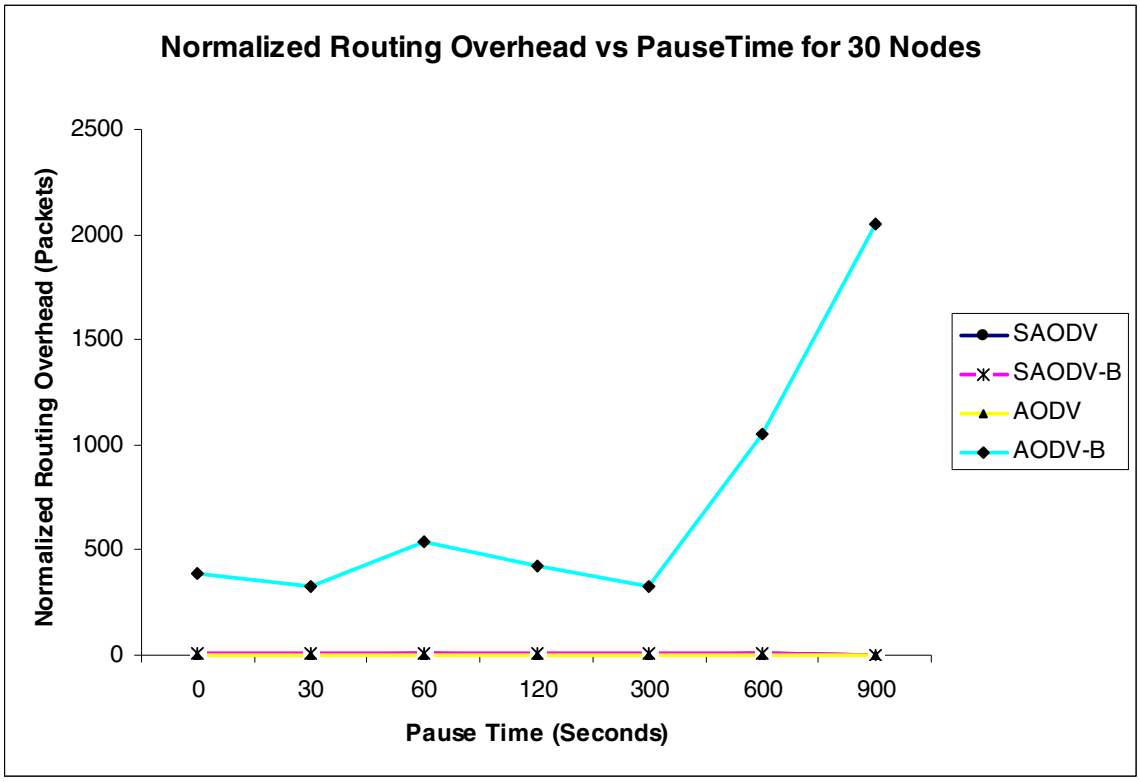

Figure 5.12: Normalized Routing Overhead vs. Pause time(30 Nodes).

- All the other protocols have performed better than AODV-B in this case. It is clearly seen that for this particular performance metric these protocols were behaving as expected.

40 Nodes:

Routing Overhead vs. Pause Time for 40 Nodes:

- The number of routing packets generated by SAODV-B is high compared to other protocols. This is due to the fact of malicious nodes and the protocol prevents the malicious nodes from participating in active communication.

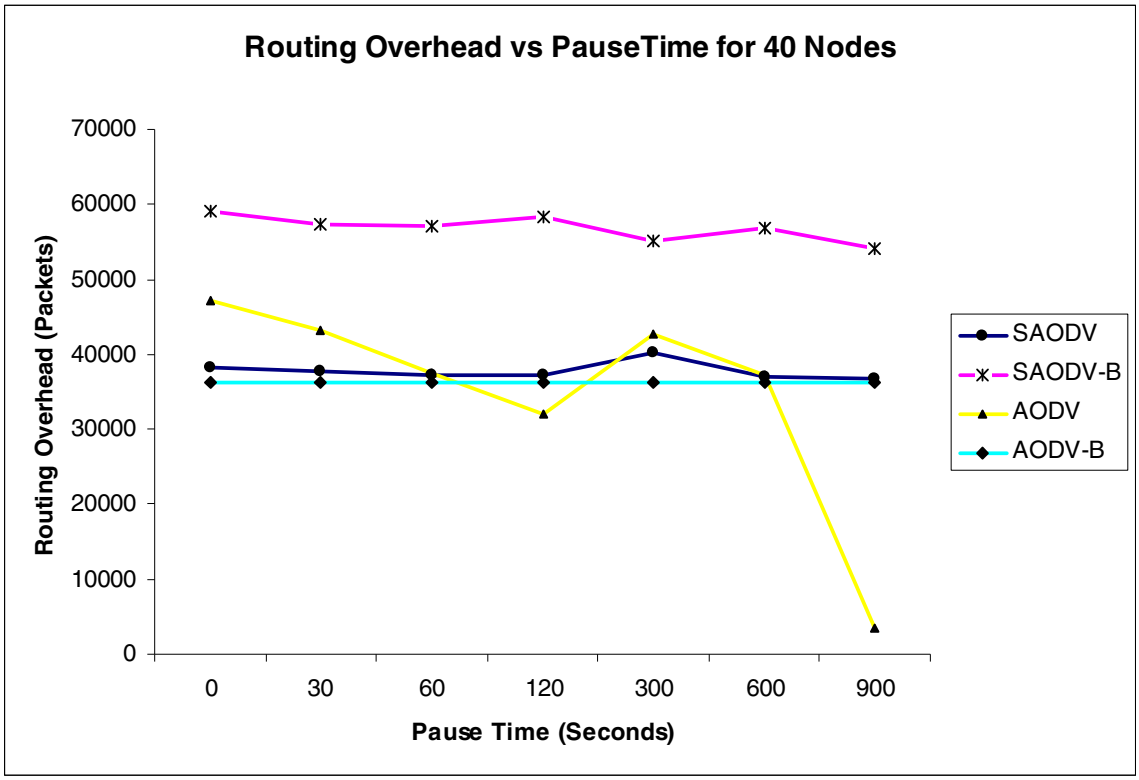

Figure 5.13: Routing Overhead vs. Pause Time (40 Nodes).

- AODV consumed the fewest number of routing packets compared to other protocols at 900 seconds. Initially the consumption of routing packets by AODV is more since due to high mobility of nodes and the consumption decreases as the pause times are increased.

Packet Delivery Fraction vs. Pause Time for 40 Nodes:

- The best performance for AODV is achieved in this scenario at 900 seconds of pause time. The PDF at 900 seconds is 99% and almost all the packets which were sent by the source were received at the destination. This is the best result which was observed and PDF on an average for AODV is approximately 90% for the entire simulations.

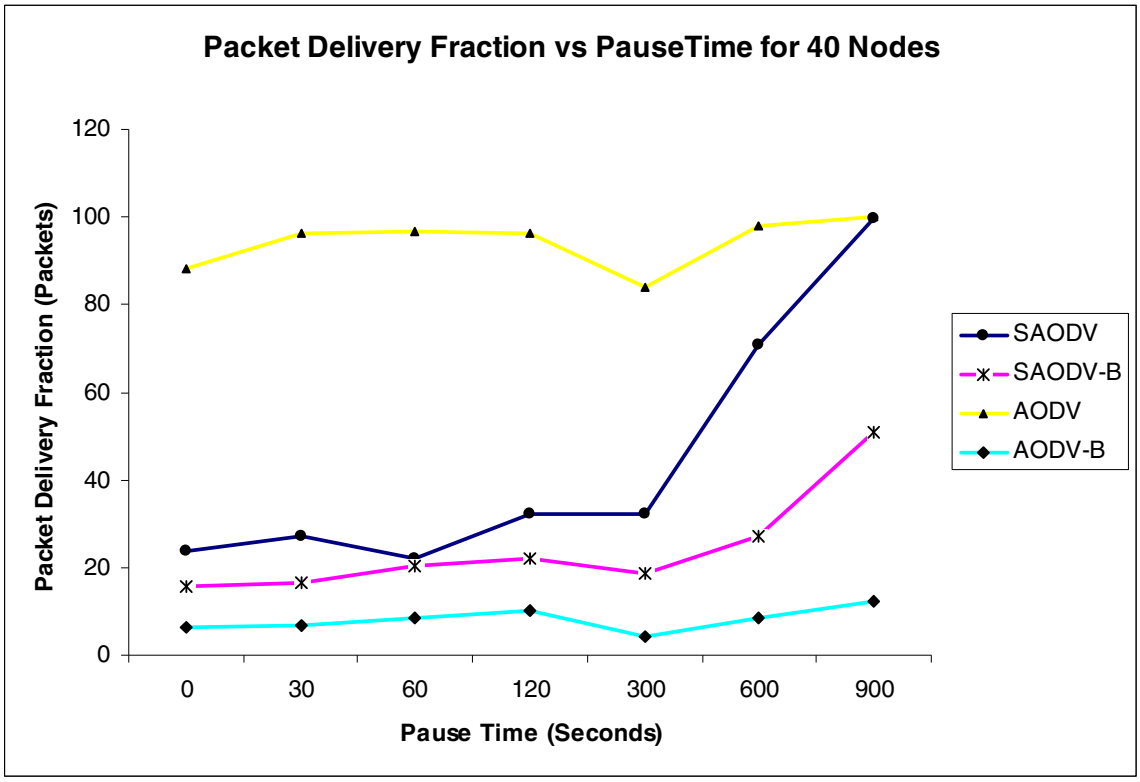

Figure 5.14: Packet Delivery Fraction vs. Pause Time (40 Nodes).

- SAODV performed somewhat better than SAODV-B in most of the scenarios.
- AODV-B had the worst performance. On average only 10% of the packets reached the destination.
- SAODV protocol has achieved its best performance of 99% even with the high routing overhead when there is no mobility in the network. It performed better than SAODV with malicious nodes in all the pause time scenarios. From this study it was evident that SAODV's performance is good when there is no mobility and the network is dense so that there are more connection pairs.

Average End-End Delay vs. Pause Time for 40 Nodes:

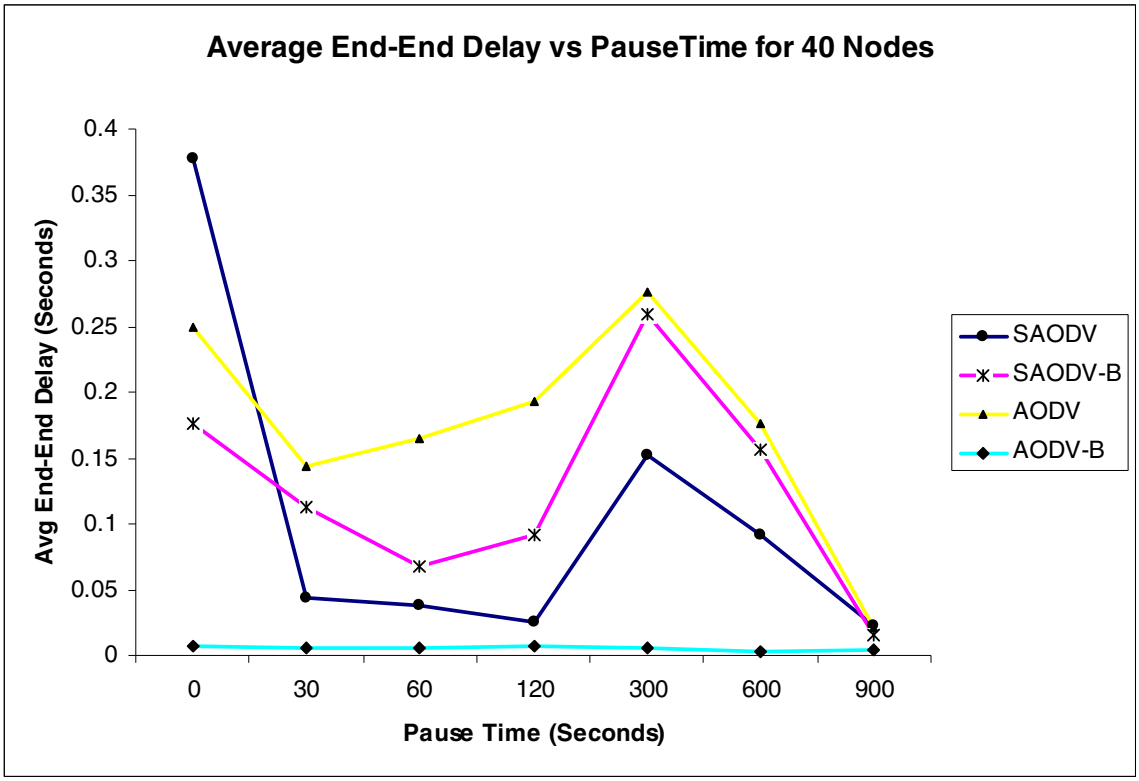

Figure 5.15: Average End-End Delay vs. Pause Time (40 Nodes).

- Delays for AODV-B routing protocol is the least since it could send only very limited number of data packets to the destination.

Normalized Routing Overhead vs. Pause time for 40 Nodes:

- Normalizing routing overhead is still high for AODV-B even under these network conditions. In some scenarios the numbers of packets sent were totally lost.
- AODV consumed fewer routing packets for each data packet which was sent to the destination as can be clearly seen from the above.
- SAODV consumed less routing packets when compared to SAODV-B.

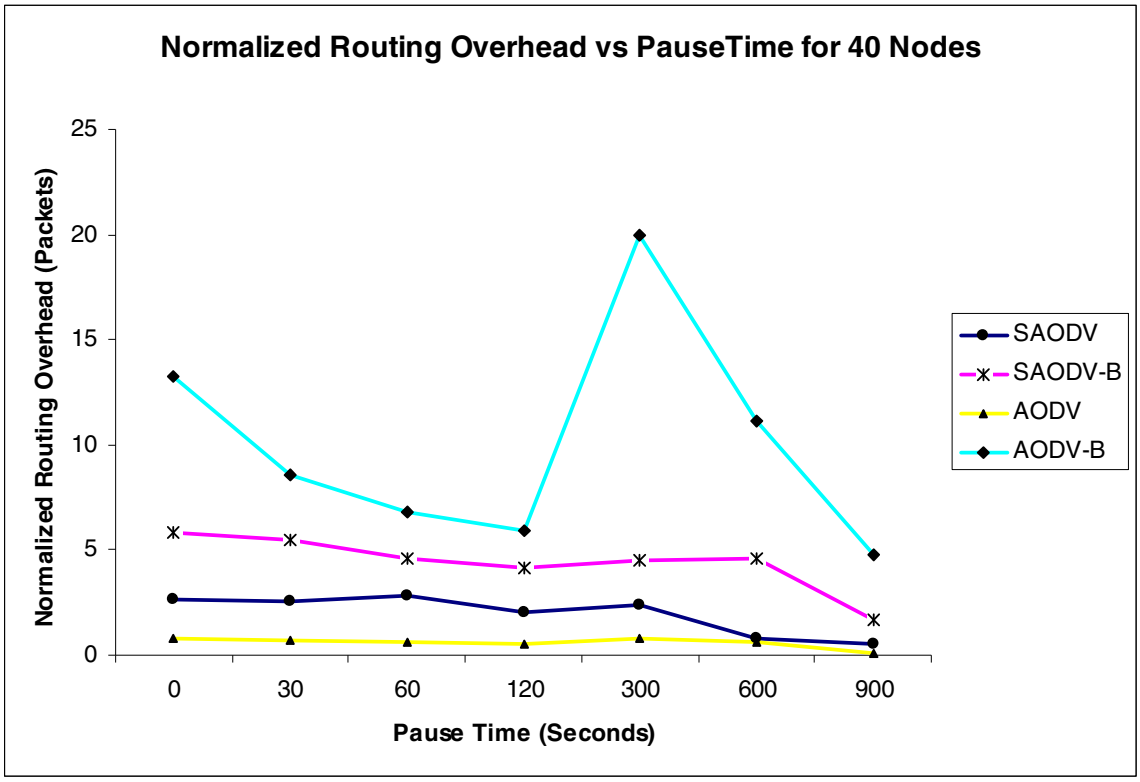

Figure 5.16: Normalized Routing Overhead vs. Pause time (40 Nodes).

All the remaining graphs which were used in the simulation part are included in the appendix section. The performances of the protocols were studied at two different speeds, namely, 1 m/s and 20 m/s for pause times 0, 30, 60, 120, 300, 600 and 900 seconds respectively.

In the above graphs for different number of nodes, the malicious nodes percentage varied from 10% to 50% of the total node population. The average of all the values was taken into consideration for the above graphs.

We next considered the performance of SAODV and AODV under different percentages of malicious node populations. For this simulation, network constraintswe re:

- Number of nodes : 30
- Number of malicious nodes : 5, 10, 15
- Pause times: 0, 30, 60, 120, 300, 600, 900 seconds.
- Network area: A rectangular field of 1500m x 500m.

For convenience protocols are represented in the following abbreviated forms:

- **SAODV-5** – Secure Ad-hoc On Demand Distance Vector Routing Protocol with 5 malicious nodes out of the total 30 nodes
- **SAODV-10** – SAODV with 10 malicious nodes.
- **SAODV-15** – SAODV with 15 malicious nodes.
- **AODV-5** – Ad-hoc On Demand Distance Vector Routing Protocol with 5 malicious nodes
- **AODV-10** – AODV with 10 malicious nodes.
- **AODV**-15 – AODV with 15 malicious nodes.

30 Nodes:

Routing Overhead vs. Pause Time for 30 Nodes:

- Routing overhead for SAODV with 15 malicious nodes was observed to be high because the more malicious nodes in the network, more work is needed in order to avoid the malicious nodes from participating in the routing. AODV has almost the same routing overhead for all the malicious node populations since it doesn't employ any measures to prevent them from participating.
- SAODV with 5 and 10 malicious nodes respectively has almost the same routing overhead.

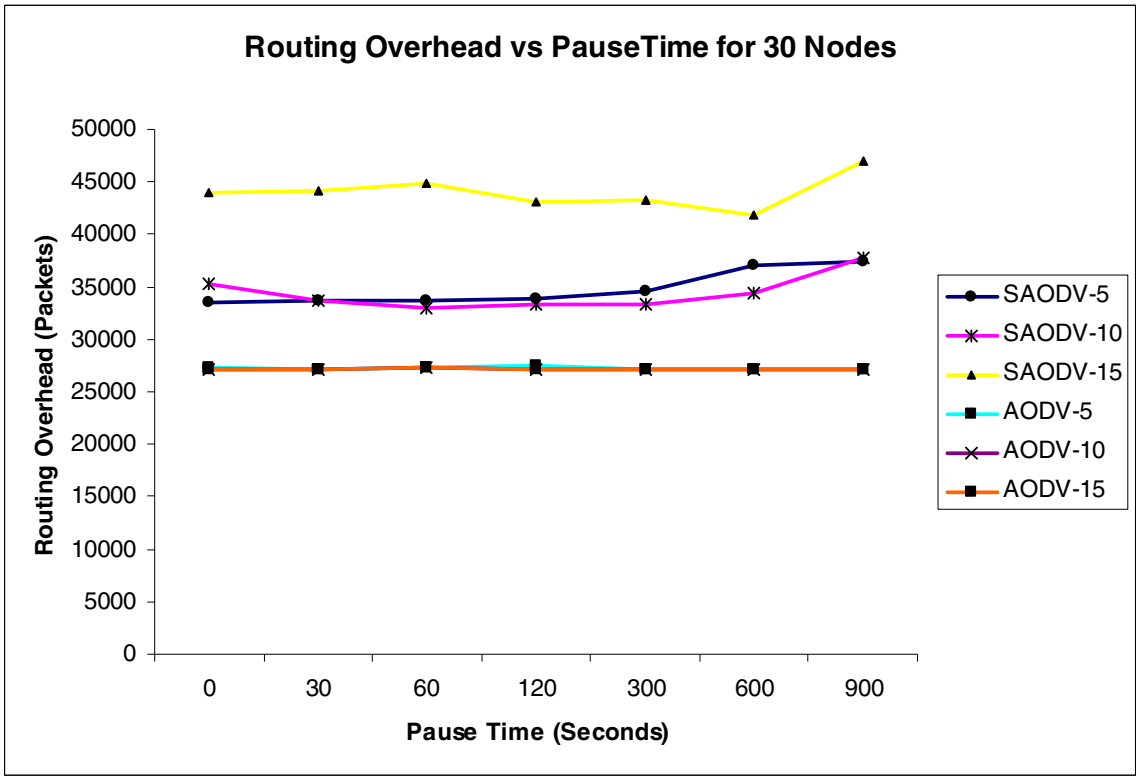

Figure 5.17: Routing Overhead vs. Pause Time (30 Nodes)

Packet Delivery Fraction vs. Pause Time for 30 Nodes:

- SAODV-5 performed well in this case compared to SAODV-10 and SAODV-15 routing protocols. PDF ratio decreases if there are more malicious nodes in the network. The same principle is applied to the AODV routing protocols.

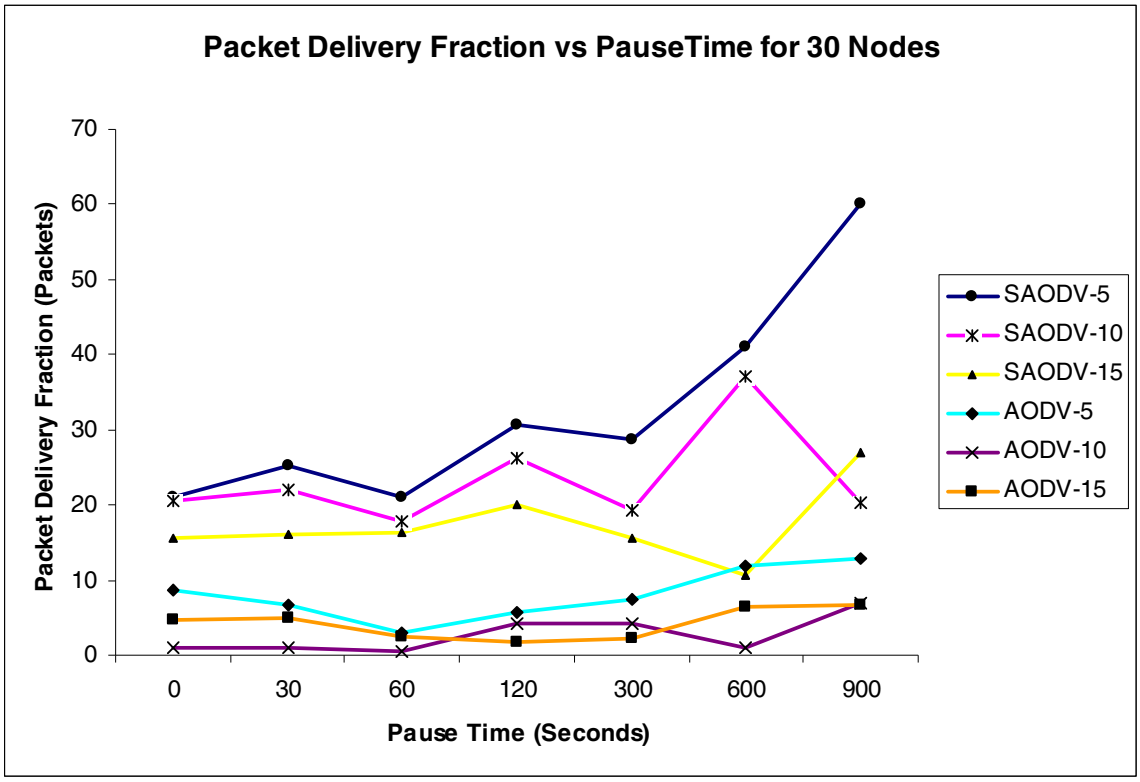

Figure 5.18: Packet Delivery Fraction vs. Pause Time (30 Nodes)

Average End-End Delay vs. Pause Time for 30 Nodes:

- Delays for the SAODV routing protocol are very high compared to AODV routing protocols since AODV routing protocols with malicious nodes can send very few number of data packets to the destination.

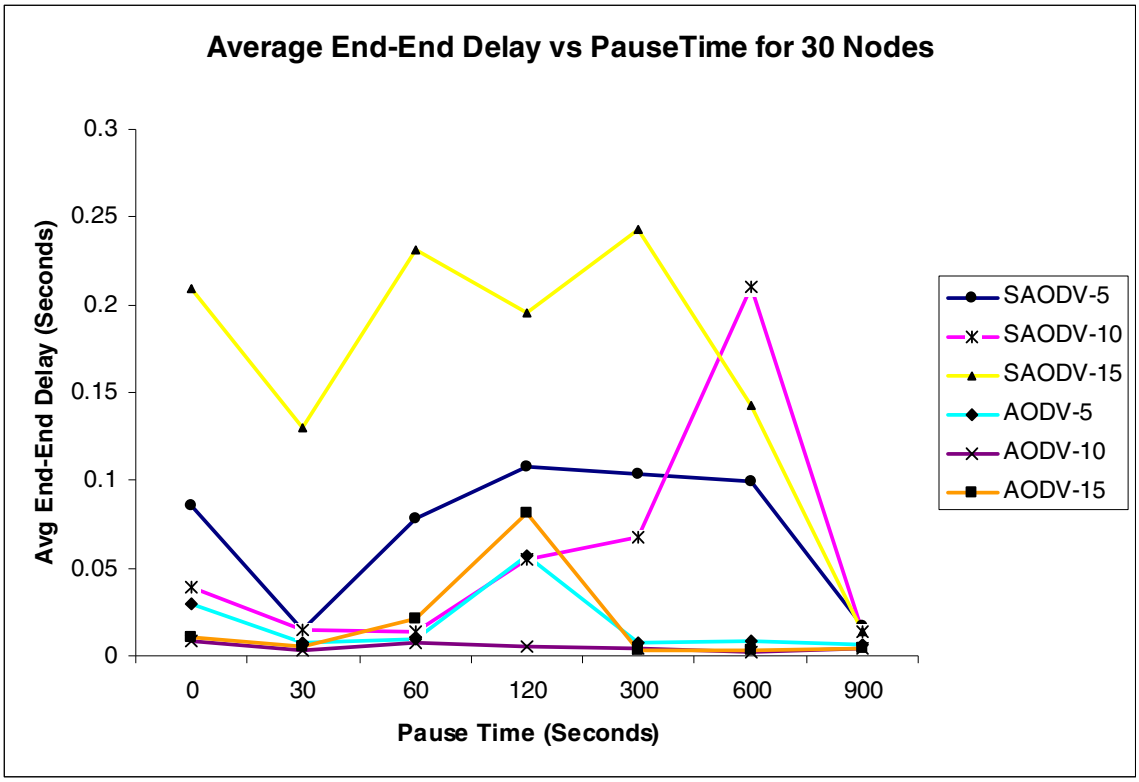

Figure 5.19: Average End-End Delay vs. Pause Time (30 Nodes).

Normalized Routing Overhead vs. Pause time for 30 Nodes:

- The Normalizing routing overhead is high for AODV routing protocols with malicious nodes as the number of data packets reaching the destination is very low. In some scenarios the numbers of packets sent were totally lost.
- SAODV routing protocols with malicious nodes performed better than AODV routing protocols with malicious nodes since more packets were reaching the destination in SAODV routing protocols when compared to AODV routing protocols with malicious nodes. This is clearly seen in the below graph.

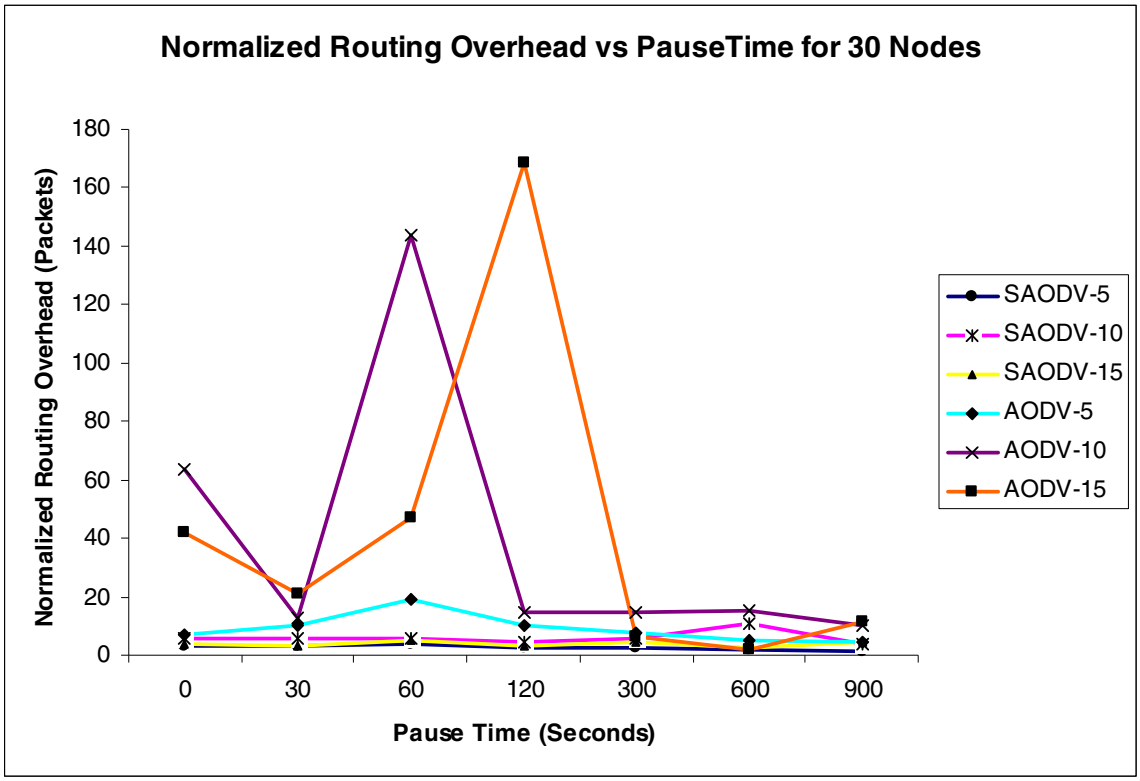

Figure 5.20: Normalized Routing Overhead vs. Pause time (30 Nodes).

CHAPTER VI

CONCLUSION AND FUTURE WORK

Out of the four protocols AODV has clearly emerged as a winner in performance when operating in the absence of malicious nodes. AODV is followed by SAODV, SAODV-B and AODV-B. AODV-B gave the worst performance in all aspects if malicious nodes were present and attacking. Secured routing protocols have more overhead than normal routing protocols as shown in the simulation when considering different conditions in the network. If security is not enabled then some heavy packet loss due to bad nodes was experienced in the network, particularly in the case of AODV-B. This thesis also investigated how the performance metrics were affected when the malicious node population varied. Safe communication is guaranteed between source and destination if security is enabled in the network. In a secured network, malicious nodes cannot participate in the active communication between source and destination.

Although SAODV can prevent many attacks, there are some attacks where SAODV will fail. A second line of defense is therefore needed to handle selfish nodes, spoofing and tunneling attacks etc., which cannot be prevented using SAODV. A real time intrusion detection protocol should be developed to monitor the changes that occur in the network and it should respond to the appropriate attacks. As future work a real time intrusion detection system should be developed and its performance should be compared with the secured and the normal versions of the routing protocols.

REFERENCES

[Boukerche 04] Azzedine Boukerche, "Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks", ACM/Kluwer Mobile Networks and Applications (MONET), Vol. 9, pp. 333-342, Aug 2004.

[Broch 98] J. Broch, D.A.Maltz, D.B. Johnson, Y.-C. Hu and J. Jetcheva, A performance comparison of multi-hop wireless ad hoc network routing protocols, *Proc. of MOBICOM'98,* pp. 85-97, October 1998.

[Corson 02] Scott Corson, "An Overview of Mobile Ad Hoc Networking", http://inet2002.org/CD-ROM/lu65rw2n/papers/t13-a.pdf, access date: October 18th 2005.

[Das 00] S.R. Das, C.E. Perkins and E.M. Royer, Performance comparison of two on-demand routing protocols for ad hoc networks, *Proc. of INFOCOM 2000*, Vol. 1, pp. 3-12, 2000.

[Deng et al. 02] Hongmei Deng, Wei Li, and D. P. Agrawal, "Routing Security in Wireless Ad hoc networks", Communications Magazine, IEEE, Vol. 10, No. 2, pp. 70-75, October 2002.

[Hass 99] Lidong Zhou and Zygmunt J. Haas, " Securing Ad Hoc Networks", IEEE Network, Vol. 13, pp. 24-30, 1999.

[Network Simulator ns2] "The Network Simulator - ns-2", http://www.isi.edu/nsnam/ns/, access date: June 15th 2005

[Perkins and Royer 99] Charles E. Perkins and Elizabeth M. Royer, “Ad hoc On-Demand Distance Vector Routing” *Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications*, pp. 90, 1999.

[UU 05] “AdHoc:ImplementationPortal”, http://core.it.uu.se/AdHoc/ImplementationPortal, access date: August 10th 2005.

[Zapata 02] Manel Guerrero Zapata and N. Asokan, " Securing ad hoc routing protocols", *Proc. International Conference on Mobile Computing and Networking*, pp. 1-10, 2002.

APPENDIX

APPENDIX A - FIGURES

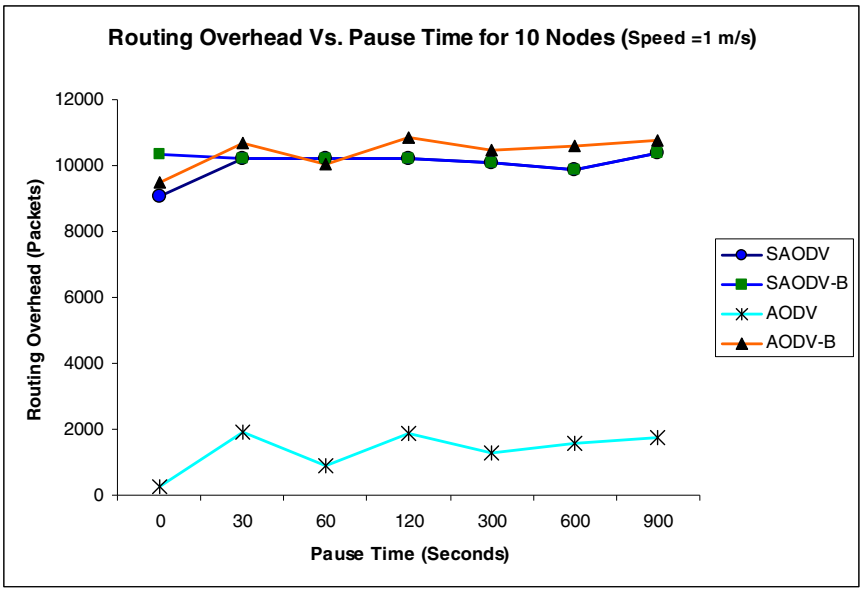

Figure A.1. Routing Overhead vs. Pause Time for 10 Nodes (Speed = 1 m/s)

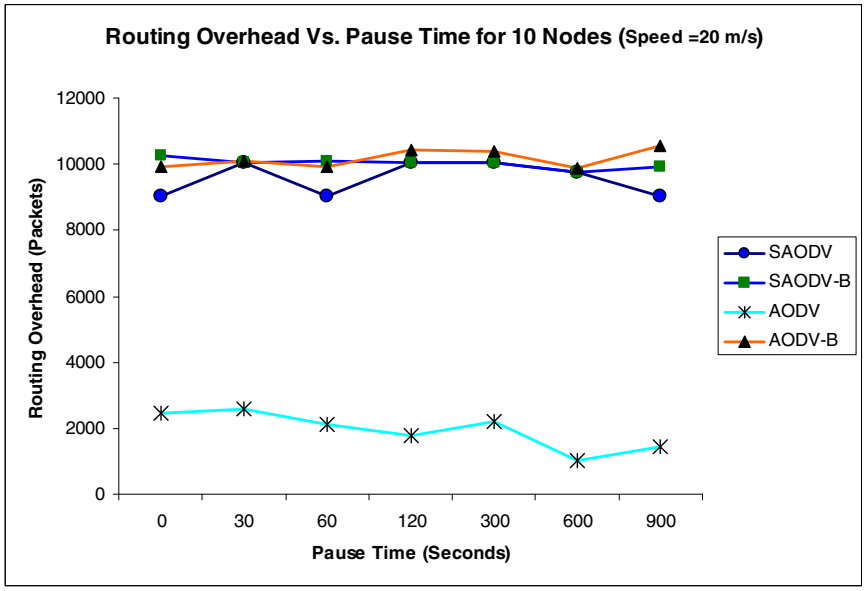

Figure A.2 Routing Overhead vs. Pause Time for 10 Nodes (Speed = 20 m/s)

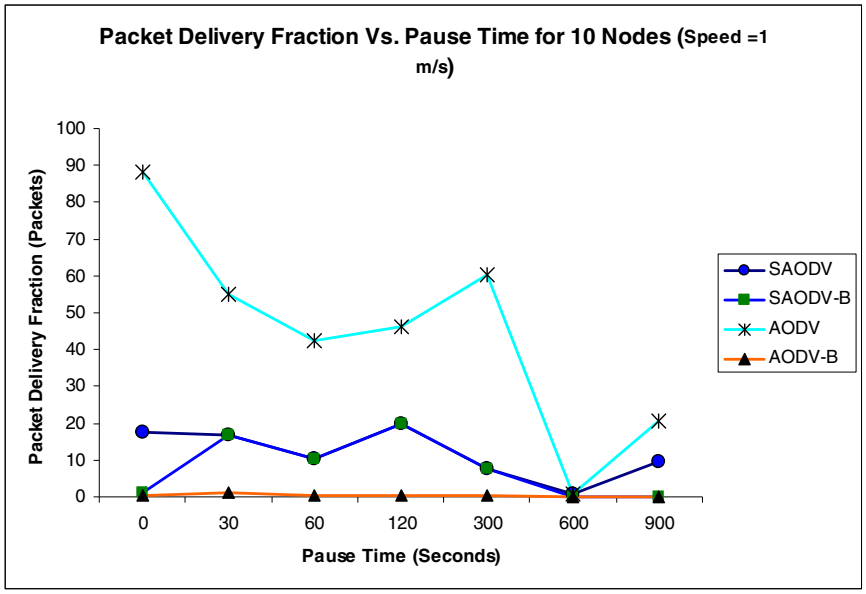

Figure A.3 Packet Delivery Fraction vs. Pause Time for 10 Nodes (Speed = 1 m/s)

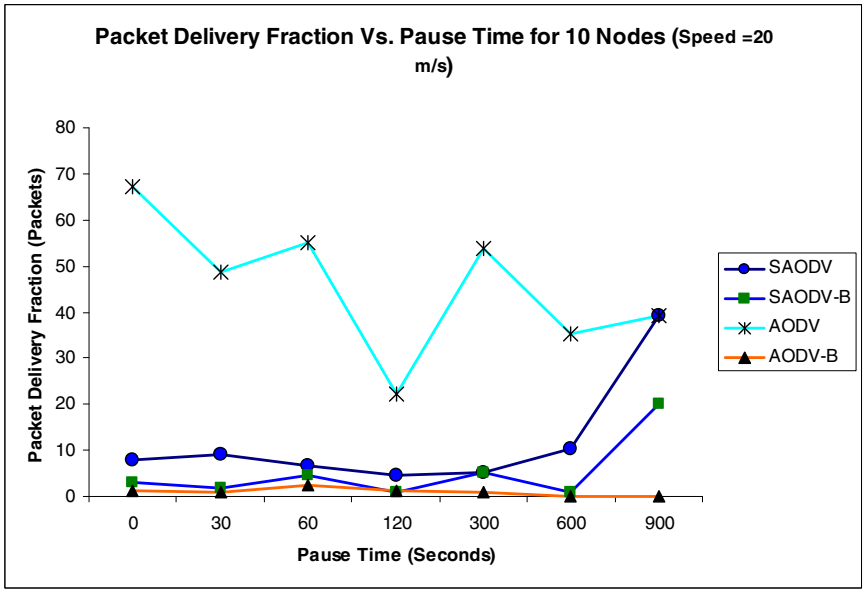

Figure A.4. Packet Delivery Fraction vs. Pause Time for 10 Nodes (Speed = 20 m/s)

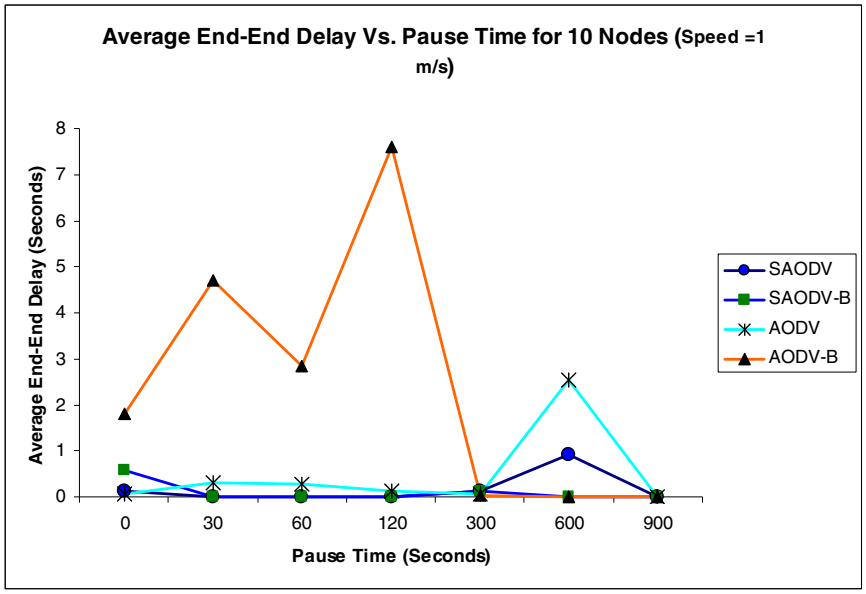

Figure A.5 Average End-End Delay vs. Pause Time for 10 Nodes (Speed =1 m/s)

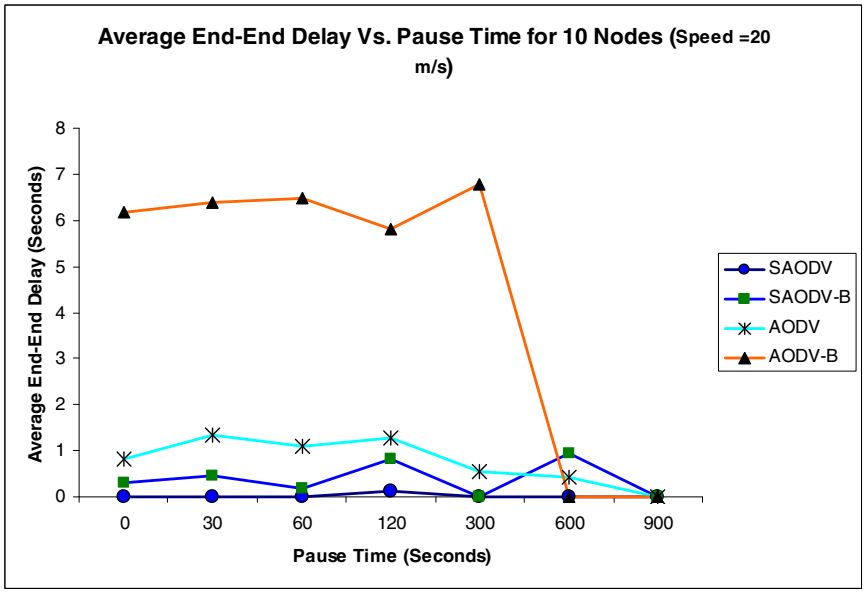

Figure A.6. Average End-End Delay vs. Pause Time for 10 Nodes (Speed =20 m/s)

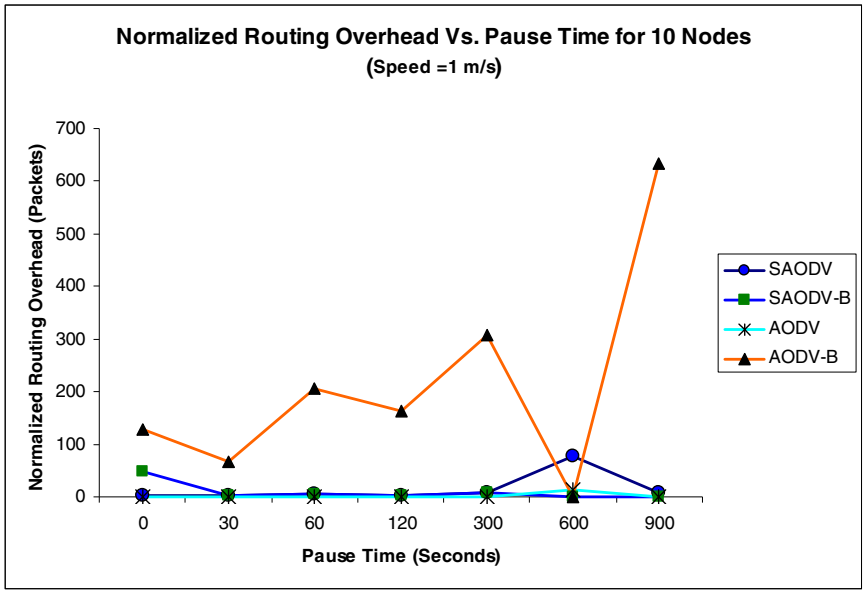

Figure A.7. Normalized Routing Overhead vs. Pause Time for 10 Nodes (Speed =1 m/s)

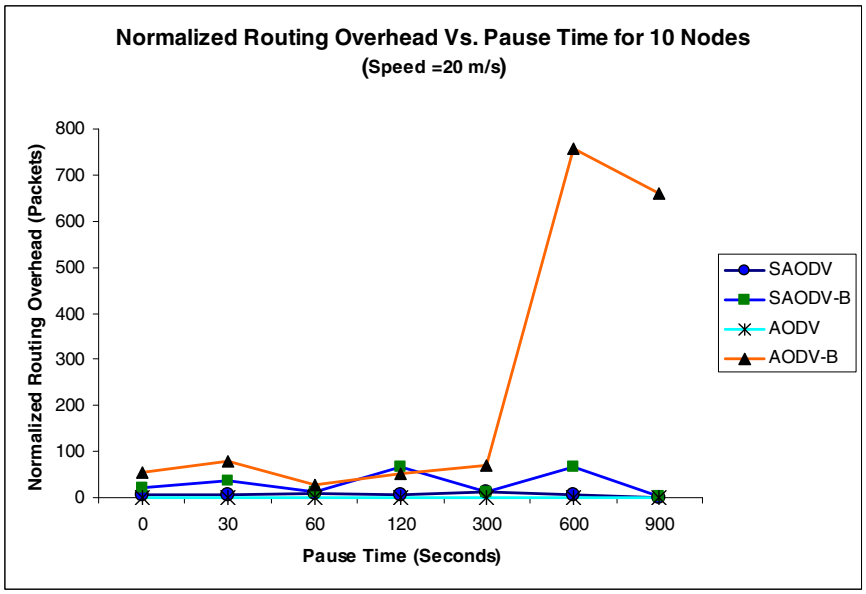

Figure A.8. Normalized Routing Overhead vs. Pause Time for 10 Nodes (Speed =20 m/s)

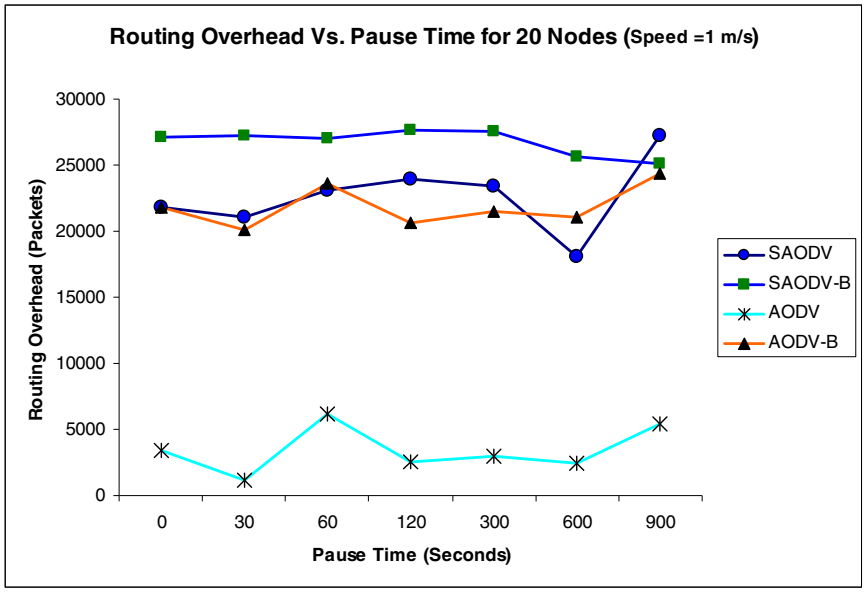

Figure A.9. Routing Overhead vs. Pause Time for 20 Nodes (Speed = 1 m/s)

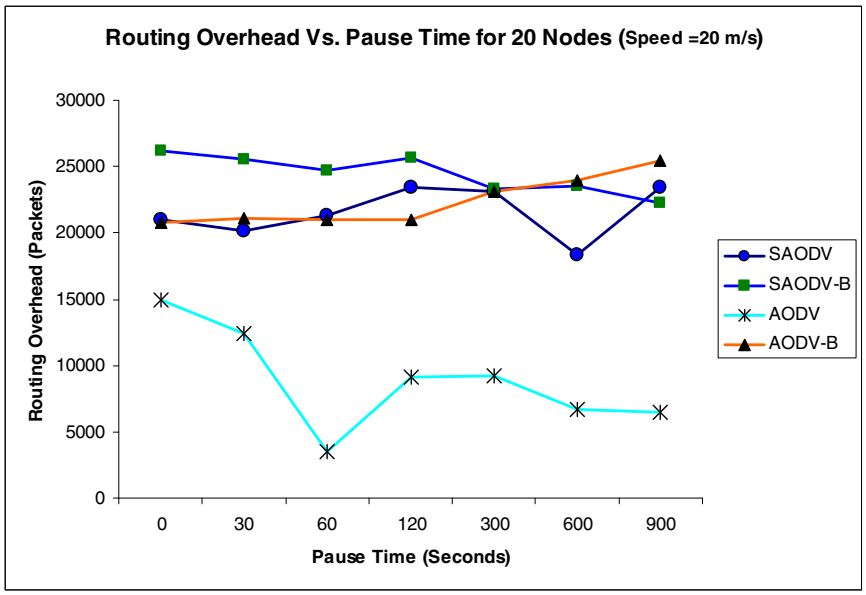

Figure A.10. Routing Overhead vs. Pause Time for 20 Nodes (Speed = 20 m/s)

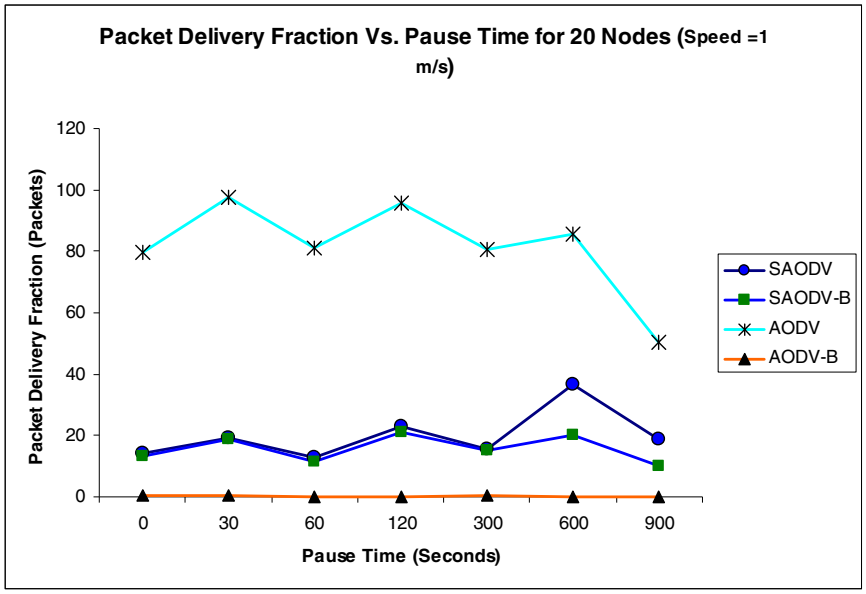

Figure A.11. Packet Delivery Fraction vs. Pause Time for 20 Nodes (Speed = 1 m/s)

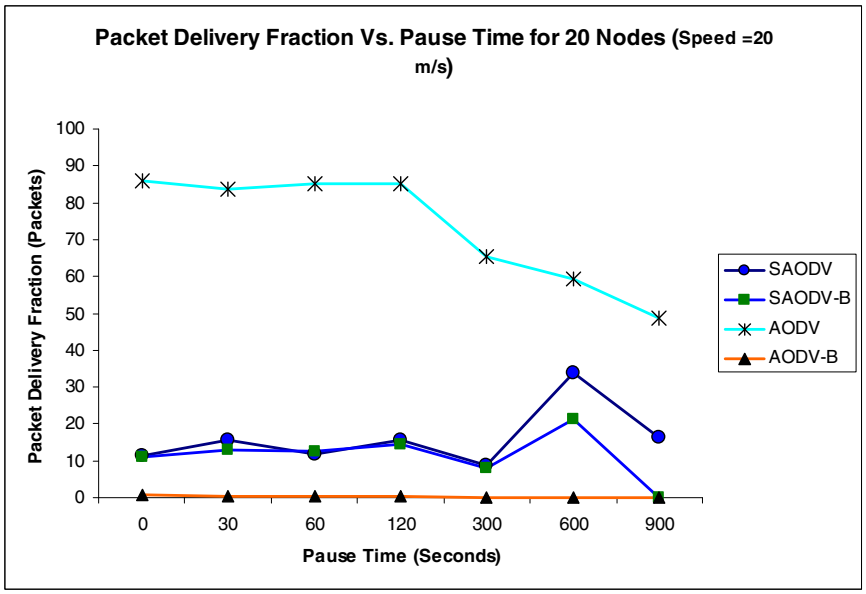

Figure A.12. Packet Delivery Fraction vs. Pause Time for 20 Nodes (Speed = 20 m/s)

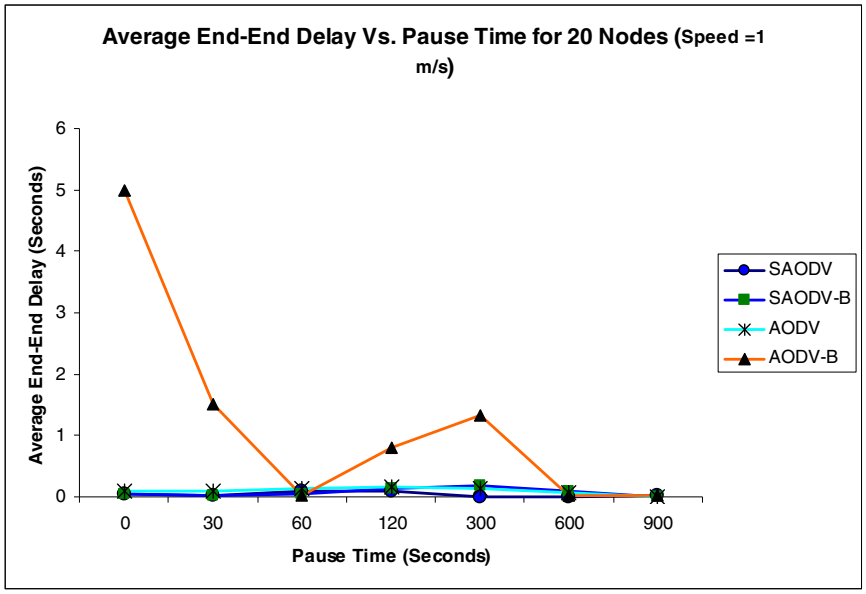

Figure A.13 Average End-End Delay vs. Pause Time for 20 Nodes (Speed =1 m/s)

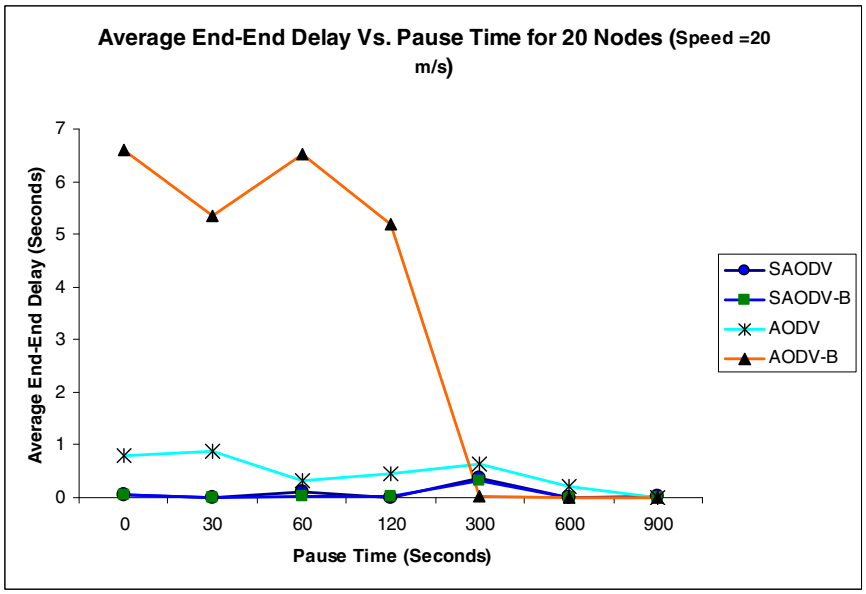

Figure A.14. Average End-End Delay vs. Pause Time for 20 Nodes (Speed =20 m/s)

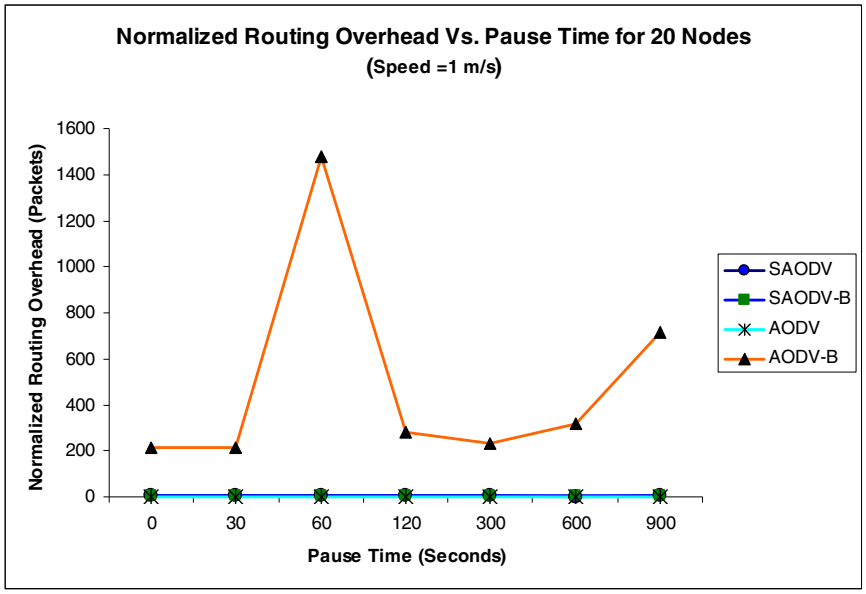

Figure A.15. Normalized Routing Overhead vs. Pause Time for 20 Nodes (Speed =1 m/s)

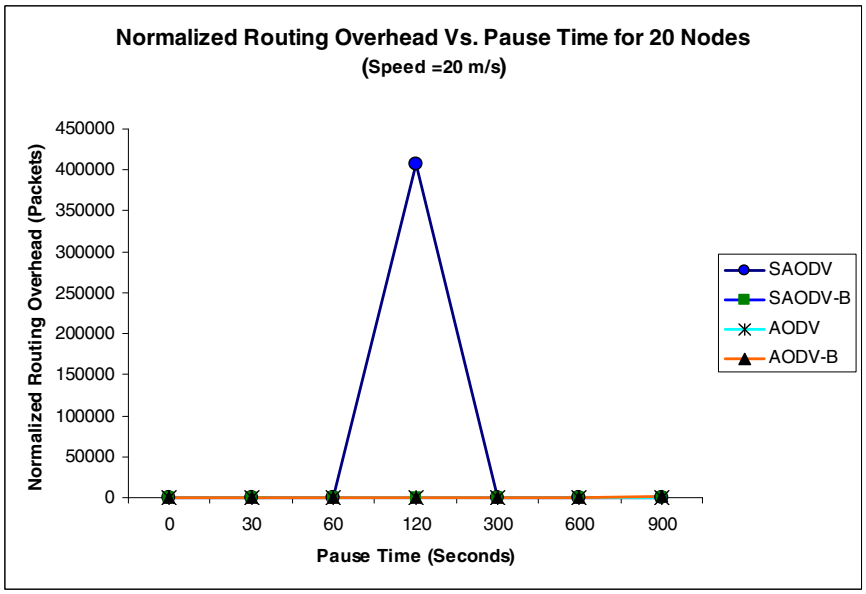

Figure A.16. Normalized Routing Overhead vs. Pause Time for 20 Nodes (Speed =20 m/s)

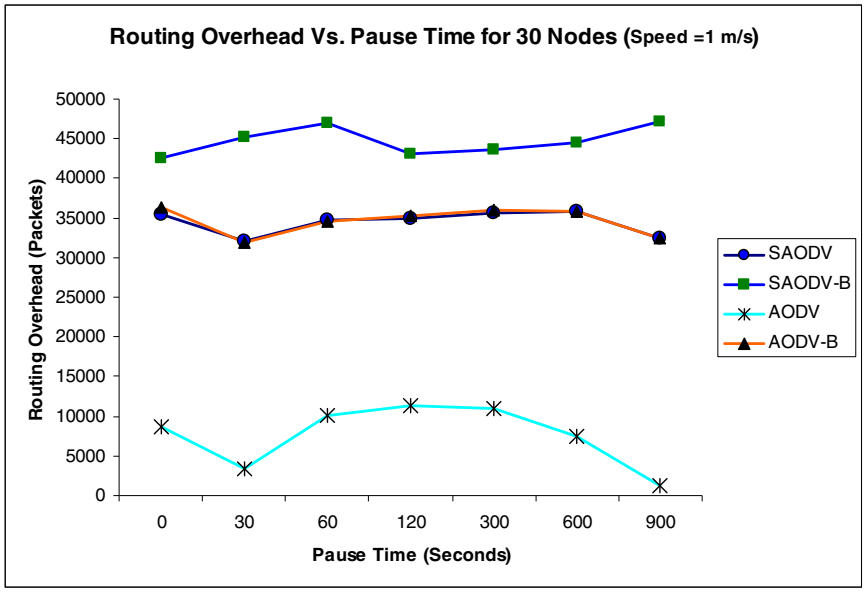

Figure A.17. Routing Overhead vs. Pause Time for 30 Nodes (Speed = 1 m/s)

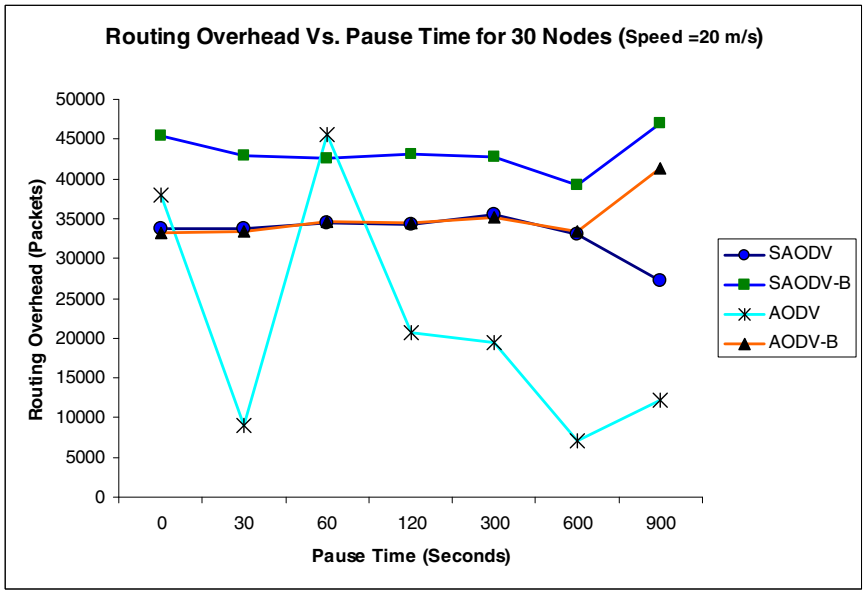

Figure A.18. Routing Overhead vs. Pause Time for 30 Nodes (Speed = 20 m/s)

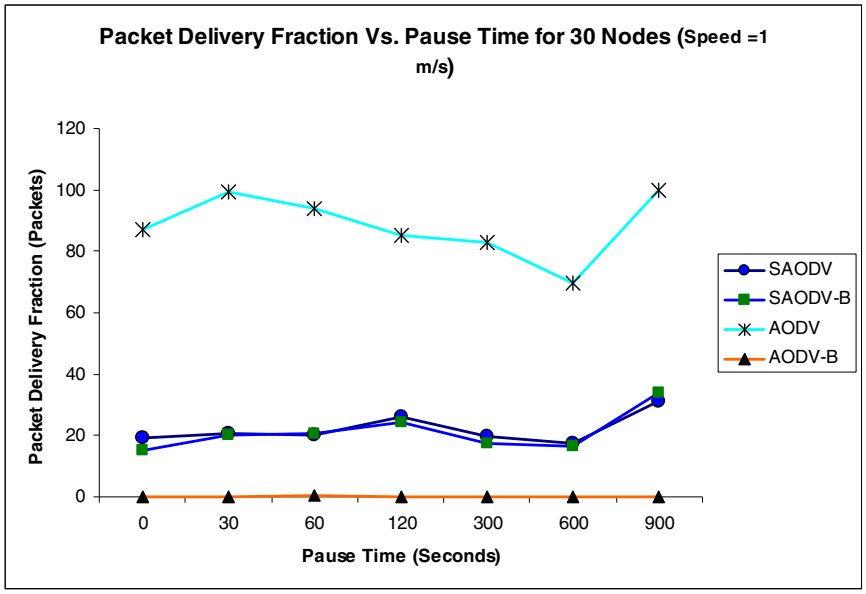

Figure A.19. Packet Delivery Fraction vs. Pause Time for 30 Nodes (Speed = 1 m/s)

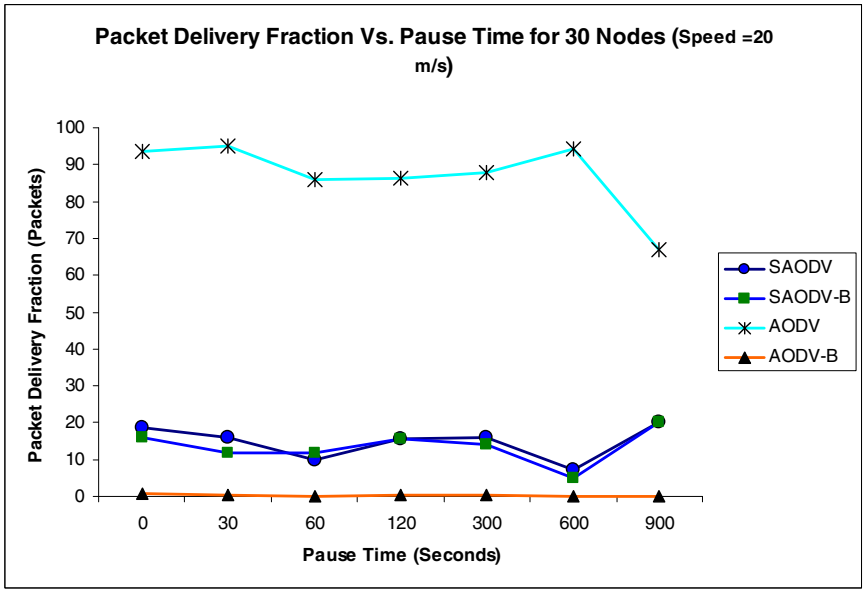

Figure A.20. Packet Delivery Fraction vs. Pause Time for 30 Nodes (Speed = 20 m/s)

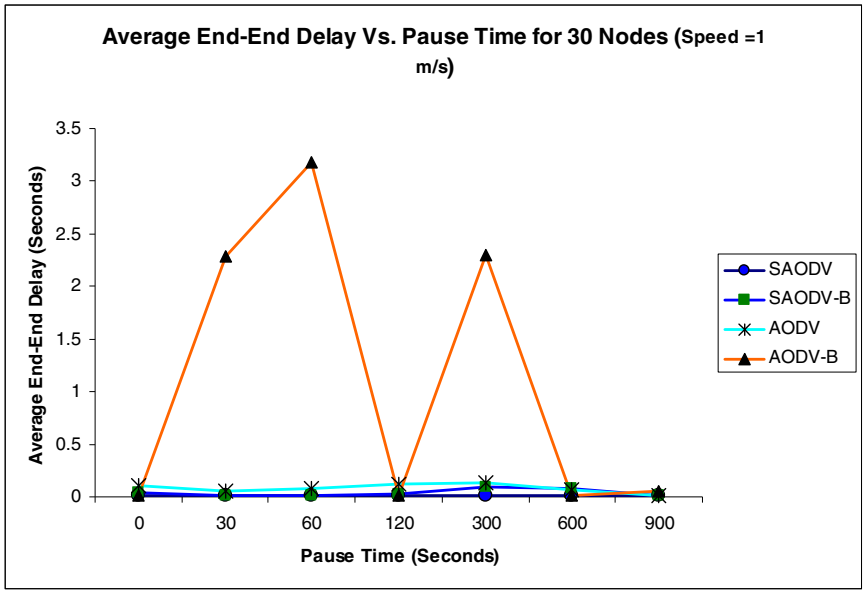

Figure A.21. Average End-End Delay vs. Pause Time for 30 Nodes (Speed = 1 m/s)

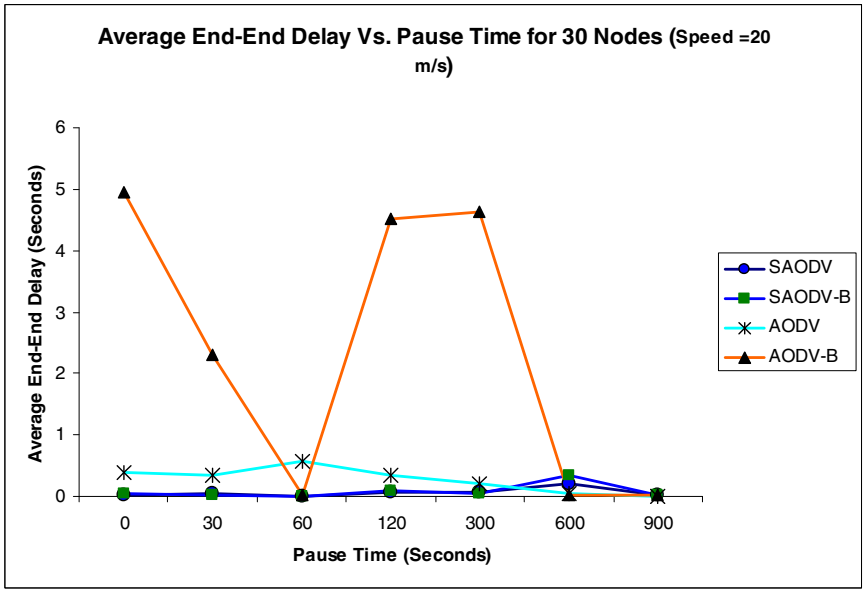

Figure A.22. Average End-End Delay vs. Pause Time for 30 Nodes (Speed = 20 m/s)

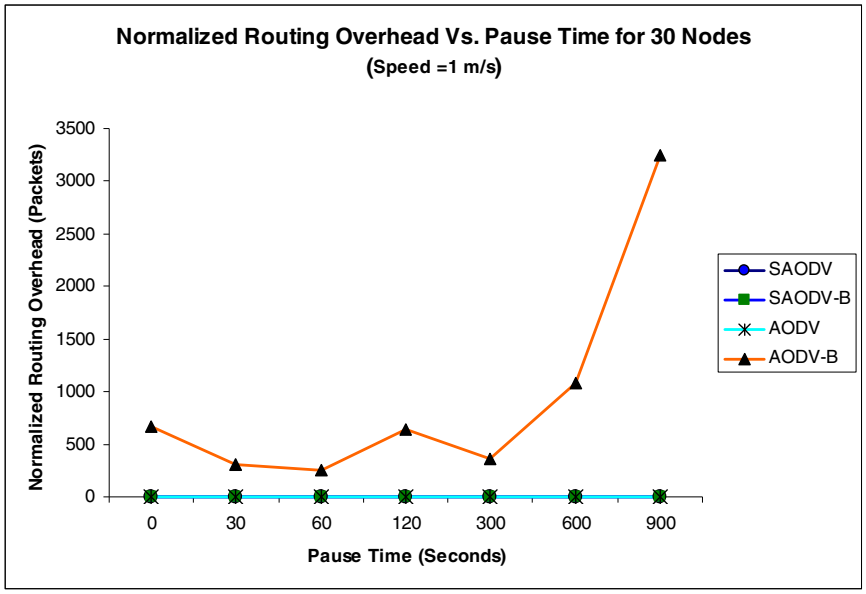

Figure A.23. Normalized Routing Overhead vs. Pause Time for 30 Nodes (Speed =1 m/s)

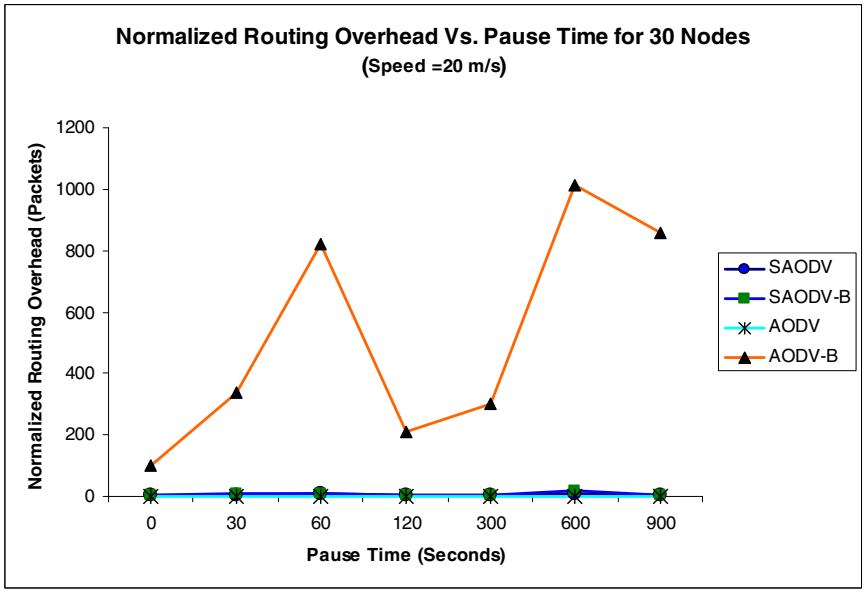

Figure A.24. Normalized Routing Overhead vs. Pause Time for 30 Nodes (Speed =20 m/s)

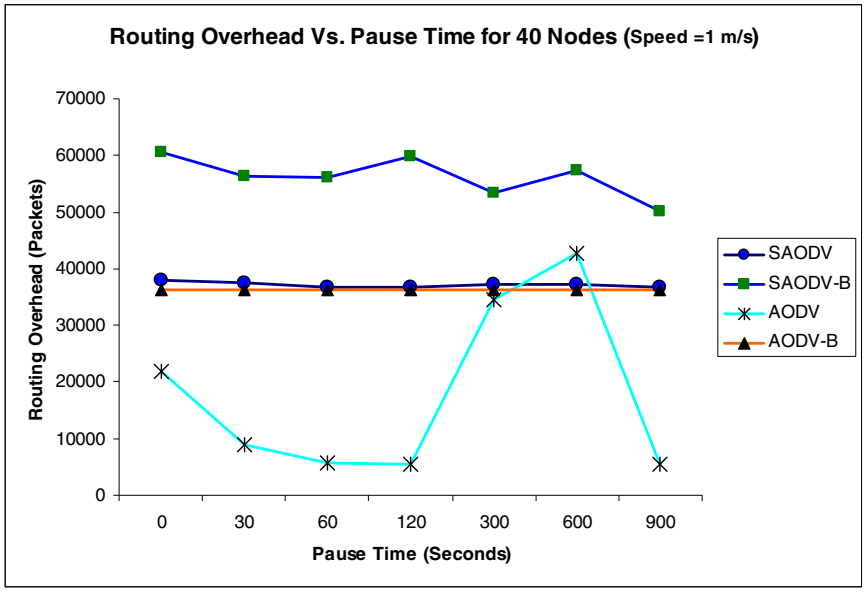

Figure A.25. Routing Overhead vs. Pause Time for 10 Nodes
(Speed = 1 m/s)

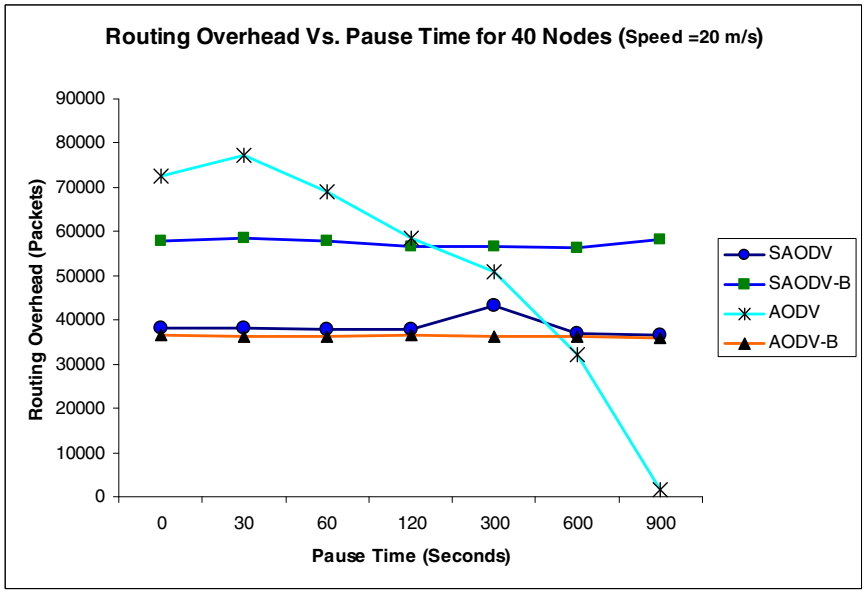

Figure A.26. Routing Overhead vs. Pause Time for 40 Nodes
(Speed = 20 m/s)

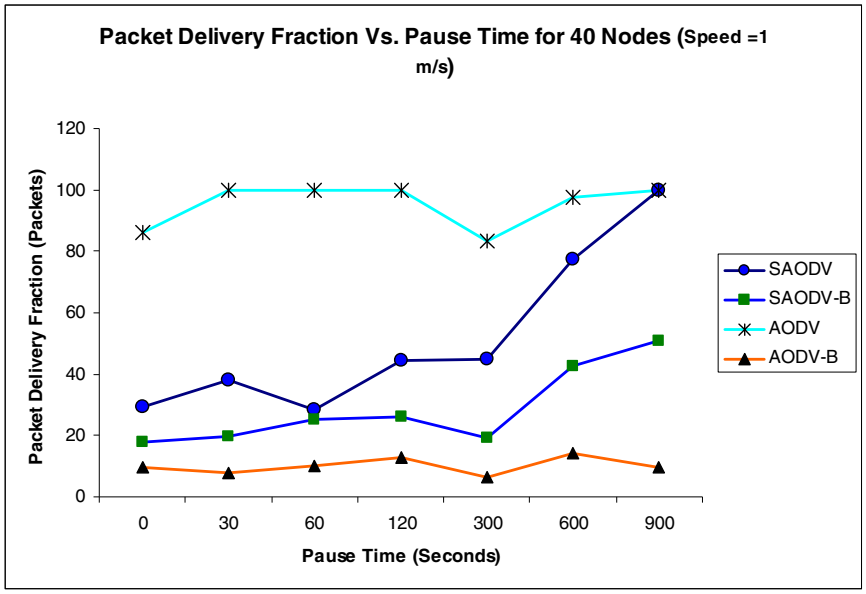

Figure A.27. Packet Delivery Fraction vs. Pause Time for 40 Nodes (Speed = 1 m/s)

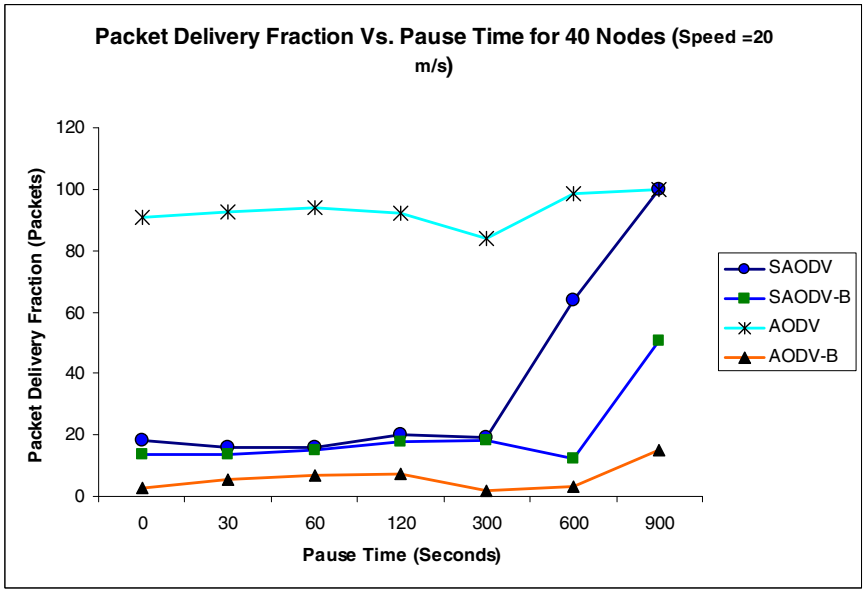

Figure A.28. Packet Delivery Fraction vs. Pause Time for 40 Nodes (Speed = 20 m/s)

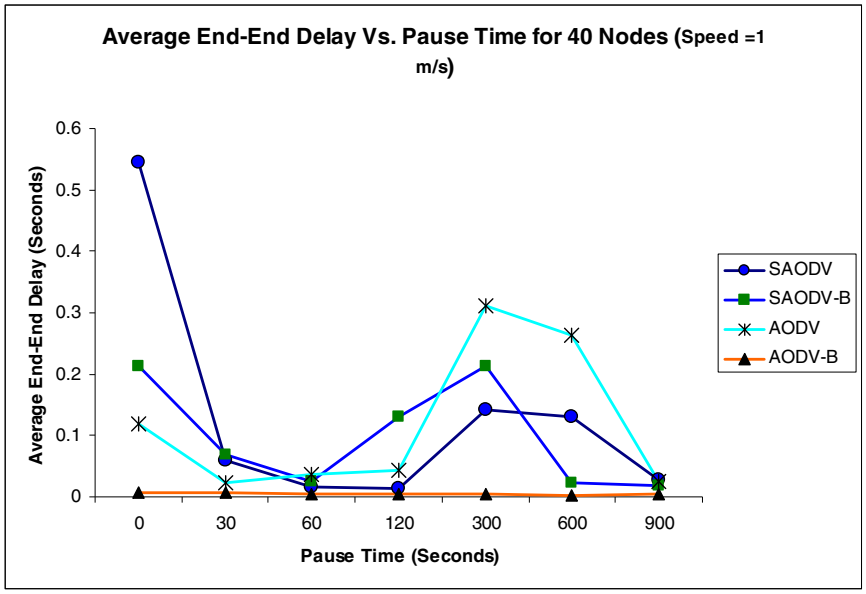

Figure A.29. Average End-End Delay vs. Pause Time for 10 Nodes (Speed =1 m/s)

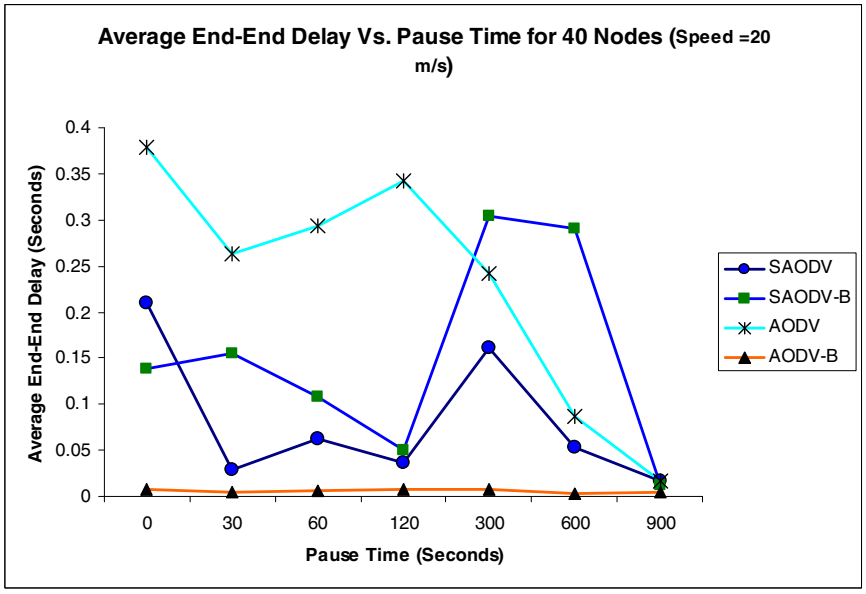

Figure A.30. Average End-End Delay vs. Pause Time for 10 Nodes (Speed =20 m/s)

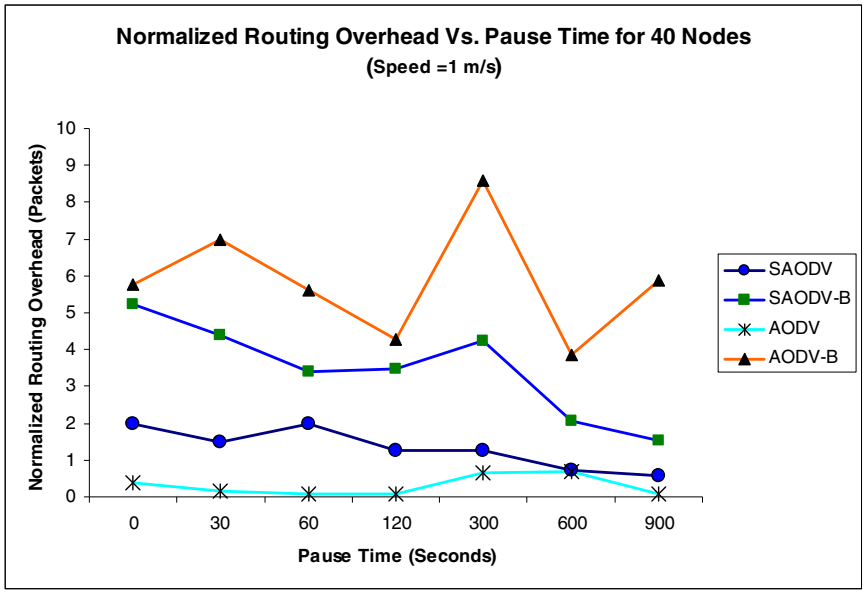

Figure A.31. Normalized Routing Overhead vs. Pause Time for 40 Nodes (Speed =1 m/s)

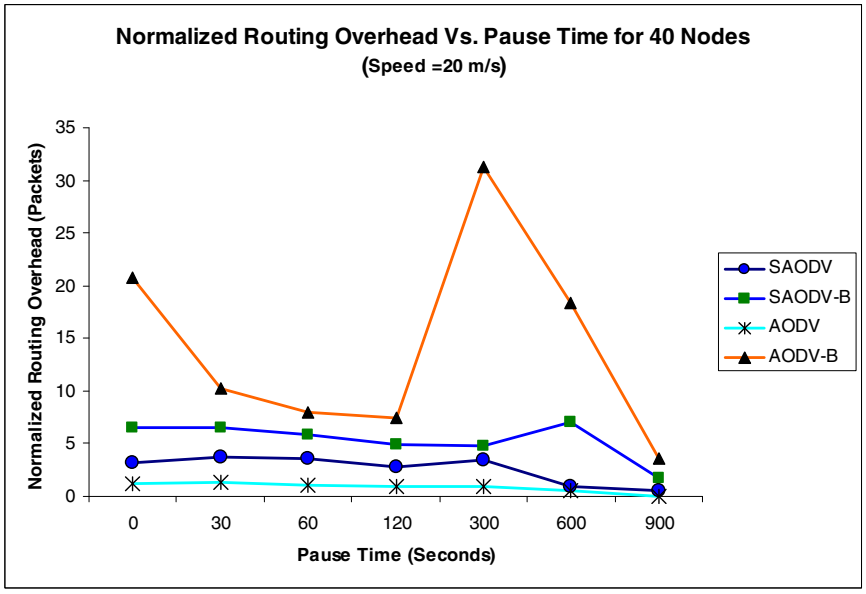

Figure A.32. Normalized Routing Overhead vs. Pause Time for 40 Nodes (Speed =20 m/s)

VITA

Dheeraj Babu Gulluru

Candidate for the Degree of

Master of Science

Thesis: PERFORMANCE EVALUATION OF A SECURED AD-HOC ROUTING PROTOCOL

Major Field: Computer Science

Biographical:

Personal Data: Born in Nellore, Andhra Pradesh, INDIA, April 13, 1981, son of Mr. Haranath Babu Gulluru and Mrs. Koteswari Gulluru.

Education: Received the degree of Bachelor of Technology in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad, India, in May 2002; completed the requirements for the Master of Science degree at the Computer Science Department at Oklahoma State University, Stillwater, Oklahoma, in May 2006.

Experience: Research Assistant in the Department of Physical Chemistry, Oklahoma State University from August 2003 to December 2005.

Professional Memberships: Association for Computing Machinery.

Name: Dheeraj Babu Gulluru Date of Degree: May, 2006.

Institution: Oklahoma State University Location: Stillwater, Oklahoma

Title of Study: Performance Evaluation of a Secured Ad-hoc Routing Protocol

Pages in Study: 73 Candidate for the Degree of Master of Science

Major Field: Computer Science

Scope and Method of Study: The purpose of this research is to find out how security affects the performance of an ad-hoc routing protocol. To study the impacts, an existing ad-hoc routing protocol AODV has been chosen and its performance is evaluated under different network scenarios. Various attack scenarios which can affect the performance were simulated and secure measures were deployed to handle such attacks. The primary objective is to find out how the routing overhead and other performance metrics were affected when additional security is added to AODV. Four different versions of the AODV protocol were simulated namely, the normal AODV routing protocol, AODV with malicious nodes, secure AODV with no malicious nodes and secure AODV with malicious nodes. These four protocols were tested on different network scenarios and their performance was evaluated.

Findings and Conclusion: The simulations were performed using the network simulator ns-2 by varying the node population, pause times and speed of the node movement in a rectangular field of 1500m x 500m. Performance metrics such as packet delivery ratio, average end-end delay and normalized routing overhead were measured along with the routing overhead for all the routing protocols. The AODV protocol performed best in the absence of malicious nodes. In the absence of malicious nodes secure AODV's performance is slightly better than secure AODV with malicious nodes. However, in the presence of malicious nodes, AODV has the worst performance compared to all the other three protocols. In other words, SAODV performs best when the network is under attack. The simulations also proved that if the node population increases then the performance of the protocols is improved due to the participation of more nodes in the routing.

ADVISER'S APPROVAL: Johnson P Thomas