Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# MANET: Security Issues and Behavior Analysis of Routing Protocol Using NS-2

**Raj Singh,** Mtech CSE, **Dinesh Kumar**
Dept. of Computer sci. & Engineering, Shri Ram College of Engineering and Management, Palwal, Affiliated to M.D.U Rohtak,
Haryana, India

***Abstract- A mobile ad hoc network (MANET) is formed with wireless mobile devices (nodes) without the need for existing network infrastructure. Security design in MANET (Mobile advoc network) is complicated because of its features including lack of infrastructure, mobility of nodes; dynamic topology and open wireless medium .Due to this MANET suffer from many security vulnerability. To enhance the security, it is very important to rate the other node which is trustworthy .An analysis of the tradeoffs between performance and security is done to gain an insight into the applicability of the routing protocols by using simulation tool NS-2 which is the main simulator. Hence a unified trust management security scheme is used. In trust management security scheme, the trust model has two components: direct observation and indirect observation. In direct observation, trust value is calculated from an observer node to observed node. On the other hand, indirect observation is also referred as secondhand information which is obtained from neighbor nodes of the observer node; the trust value is calculated between them. By combining these two components in the trust model, a more accurate trust value is obtained. This will help to improve throughput and packet delivery ratio in the network.***

***Keywords— MANET, Security, Trust Management.***

## I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes and connected in dynamic manner. Nodes forming a temporary/short-lived network without any fixed infrastructure where all nodes are free to move about arbitrarily. Nodes must behave as routers, take part in discovery and maintenance of routes to other nodes in the network.[1] Wireless links in MANET are highly error prone and can go down frequently due to mobility of nodes. Stable routing is a very critical task due to highly dynamic environment in Mobile Ad-hoc Network. So mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which . form a random topology. The routers are free to move randomly and organize themselves at random. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced disasters, military conflicts, emergency medical situations. The general issues in ad hoc wireless networks are then discussed, followed by a few interesting applications. The final section gives an outline of the chapters to follow.

## II. DESIGNING ISSUES IN MANET

The following design issues must be considered before designing a routing protocol for MANETs [1]- Mobile Ad-hoc Network are highly dynamic in nature and no fixed infrastructure in these type of network. Due to this, issues in designing Mobile Ad-hoc Networks using a routing protocol are explain as :

### *A. Error-prone channel state*

The characteristics of the links in a wireless network typically vary, and this calls for an interaction between the routing protocol, if necessary, find alternate routes.[4]

### *B. Hidden problem*

Node A and node C are in range for communicating with node B, but not with each other. In the event that both try to communicate with node B simultaneously, A and C might not detect any interference on the wireless medium. Thus, the signals collide at node B, which in turn will be unable to receive the transmissions from either node. The typical solution for this so-called “Hidden terminal” problem is that the nodes coordinate transmissions themselves by asking and granting permission to send and receive packets. This scheme is often called RTS/CTS (Request To Send/Clear To Send).The basic idea is to capture the channel by notifying other nodes about an upcoming transmission. This is done by stimulating the receiving node to output a short frame so that nearby nodes can detect that a transmission is going to take place. The nearby nodes are then expected to avoid transmitting for the duration of the upcoming (large) data frame.

 

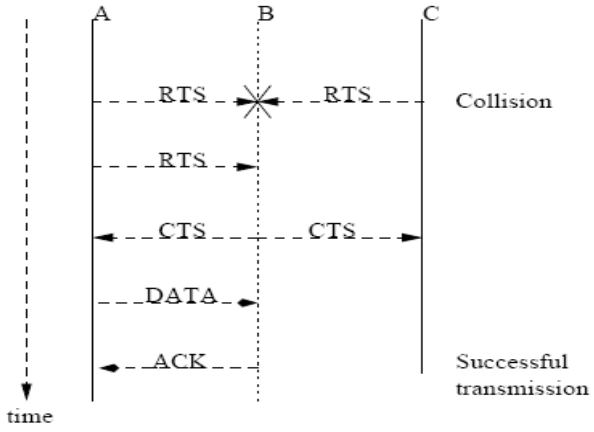


Figure 2.1: The Hidden Terminal Problem

This problem occurs in networks using contention based protocols such as ALOHA, CSMA/CD, etc. When two nodes which are out of range of each other send data frames to a node which is within their respective radio ranges, a collision of data frames occurs. As shown in Figure.2.1, when both nodes A and C transmit data frames to node B a collision occurs. This problem can be resolved by using a mechanism called RTS/CTS handshake [2]. The exposed node problem is shown in Figure.2.2. An exposed node is one which is in the range of the transmitter, but out of the range of the receiver. In Figure.2.2, when node C is transmitting to node D, B overhears this and is blocked. Now if node B wants to transmit to node A, it cannot do so.

***C. Exposed terminals***

Consider a topology similar to that of previous figure, but with an added node D only reachable from node C. Furthermore, suppose node B communicates with node A, and node C wants to transmit a packet to node D. During the transmission between node B and node A, node C senses the channel as busy. Node C falsely concludes that it may not send to node D, even though both the transmissions (i.e., between node B and node A, and between node C and node D) would succeed. Bad reception would only occur in the zone between node B and node C, where neither of the receivers is located. This problem is often referred to as "the exposed terminal problem". Both the hidden and the exposed terminal problem cause significant reduction of network throughput when the traffic load is high.

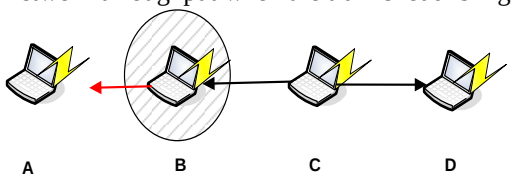


Figure 2.2: The Exposed Terminal Problem

***D. Security***

Due to on open environment where MANETs are typically deployed, the routing protocols are prone to several attacks. Further, there is also the issue of secure key distribution. This issue will be further explored further when secure routing is discussed in Chapter-4.

## III. ROUTING PROTOCOLS OF MANET

**A. Proactive protocols** In networks utilizing a proactive routing protocol, every node maintain one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node. To maintain up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis which in turn leads to relatively high overhead on the network. The advantage is that routes will always be available on request.

**B. Reactive protocols** Unlike proactive routing protocols, reactive routing protocols do not make the nodes initiate a route discovery process until a route is required. This leads to higher latency than with proactive protocols, but lower overhead

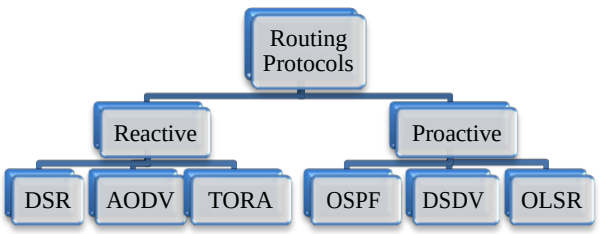


Figure 3.1: Routing protocols in MANET

 

## IV. SECURITY ATTACK IN MOBILE AD-HOC NETWORK

Security is an essential service for wired and wireless network communications. The success of mobile ad-hoc networks (MANET) strongly depends on people's confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. First, we give an overview of attacks according to the protocols stacks, and to security attributes and mechanisms. We present a different Types of Attacks Faced by Routing Protocols. Then we present preventive approaches following the order of the layered protocol stacks. We also put forward an overview of MANET intrusion detection systems (IDS). There are a wide variety of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination

**Types of Attacks Faced by Routing Protocols**

Due to their underlined architecture, ad-hoc networks are more easily attacked than a wired network. The attacks prevalent on ad-hoc routing protocols can be broadly **classified into passive and active attacks.**

**(i) A Passive Attack** does not disrupt the operation of the protocol, but tries to discover valuable information bylistening to traffic. Passive attacks basically involve obtaining vital routing information by sniffing about the network[7]. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated. Even if it is not possible to identify the exact location of a node, one may be able to discover information about the network topology, using these attacks.

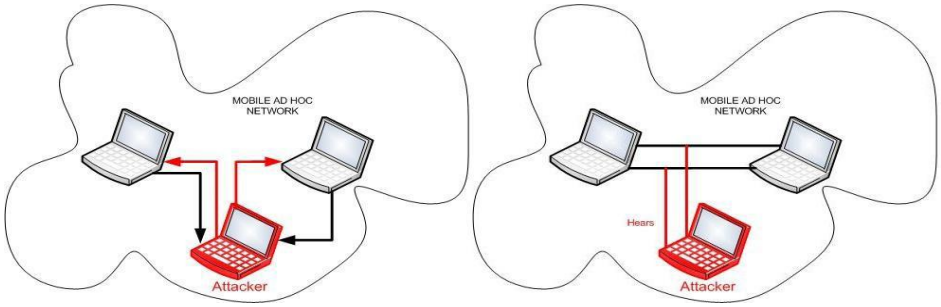


Fig. 4.1 Active and Passive Attack in MANETs

**(ii) An Active Attack**, however, injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The goal is basically to attract all packets to the attacker for analysis or to disable the network. Such attacks can be detected and the nodes can be identified.

On the basis on network protocol stack, attacks can be classified into following categories (below is a classification of security attacks based on protocol stack; some attacks could be launched at multiple layers):

a. Application layer :Repudiation, Data Corruption Attacks
b. Transport layer :Session Hijacking, SYN Flooding Attacks
c. Network layer :Wormhole, Blackhole, Byzantine, Flooding Attacks
d. Data link layer :Resource Consumption, Location Disclosure Attacks
e. Physical layer :Traffic Analysis, Monitoring, Disruption MAC (802.11)

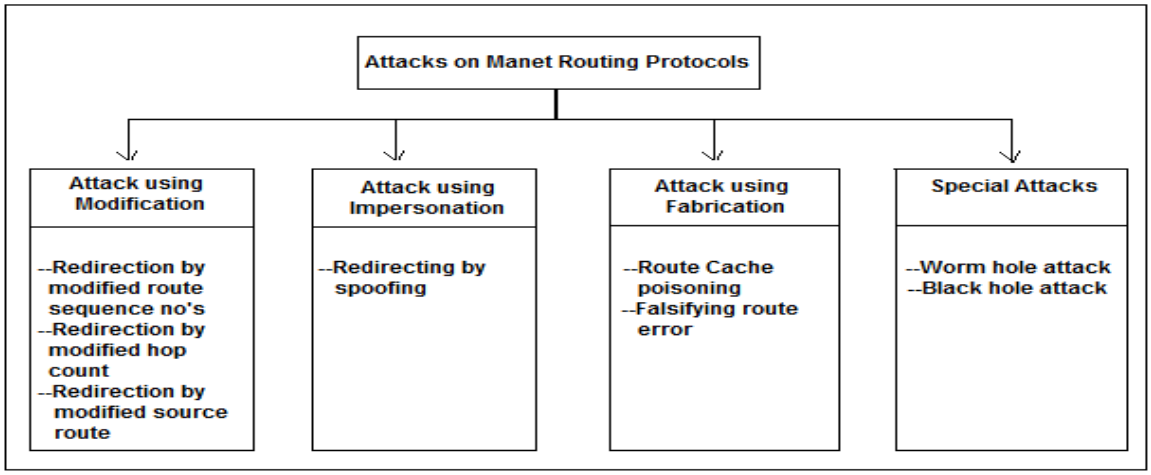


Fig 4.2 Attacks on MANET routing protocols

**(i) Attacks using Modification:**

In case of modification type of attacks some of the messages in the protocol fields are modified and then these messages passed among the nodes, due to this way it become the cause of traffic subversion, as well as traffic redirection and also act as a Denial of Service (DoS) attacks. There are some of these types of attacks are given below:

 

**A. Route sequence numbers modification:** In this type of attack which is mainly possible against the AODV protocol. In this case an attacker (i.e. malicious node) used to modify the sequence number in the route request packets.

**B. Hop count modification attack:** In this type of attacks where it is also mainly possible against the routing protocol AODV, here attacker mostly change hope count value and due to this way it will become the cause of attract traffic. They are mainly used to include new routes in order to reset the value of hop count field to a lower value of a RREQ packet or sometime even it is used to set to zero.

**C. Source route modification attack:** In this type of attack which is possible against DSR routing protocol where attacker (malicious node) modify source address and move traffic towards its own destination. In Fig. 2.6 the mechanism is defined, where the shortest path between source S and destination X is defined (S-A-B-C-D-X). Which shows that node S and the node X cannot communicate each other directly, and in the scenario where the node M which act as a malicious node which are going to attempt a denial-of-service attack. Let suppose that the node S which act as a source try to send a data packet towards the node X but if the node M intercept the packet and remove the node D from the list and the packet forward towards node C, where the node C will try tosend the picket towards the distention X which is not possible because the node C can't communicate with X directly, Due to this way the M node has successfully established a DoS attack on X.

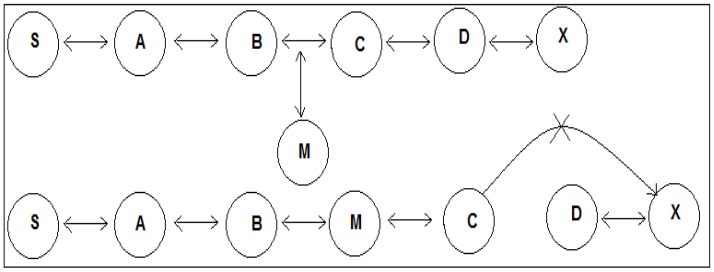


Fig. 4.3 an example of route modification attack

**(ii) Attacks using Impersonation:**

In this type of attacks where attacker is used to violates authenticity and confidentiality of a network. In this attack an attacker (i.e. malicious node) uses to impersonate the address of other user node in order to change the network topology. This type of attack can be described in the Figure 2.7 given below:

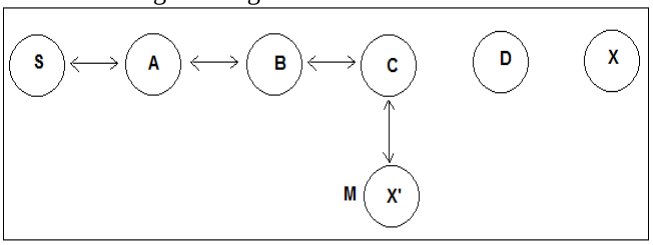


Fig. 4.4 Type of impersonation attack

In the above figure where the S node wants to send data towards the node X and before sending data to node X it starts a Route Discovery process. During route discovery process there is a malicious node M, when it receive route discovery packet regarding the node X then it modify its address and change to node X, like impersonates node X as X'. After that it send packet back to source node S that I am the destination node by RREP packet request. When the source node receives RREP packet information it doesn't authenticate node and accept the route and send data to the malicious node. This type of attacks also called routing loop attack which will become the cause of loops within the network.

**(iii) Attacks using Fabrication:**

In this type of attacks, where an attacker as a malicious node try to inject wrong messages or fake routing packets in order to disrupt the routing process. The fabrication attacks are very much difficult to detect in the mobile ad hoc network. Attacks using fabrication process are discussed very well in [20] and [21]. In Figure 2.8 where fabrication attacks is explained by an example. In the example where the source node S wants to send data towards the destination node X, so therefore at start it sends broadcast message and request for route towards the destination node X. An attacker as a malicious node M try to pretends and modify route and returns route reply to the node (S). Furthermore, an attacker's nodes use to fabricate RERR requests and advertise a link break nodes in a mobile ad hoc network by using AODV or DSR routing protocols.

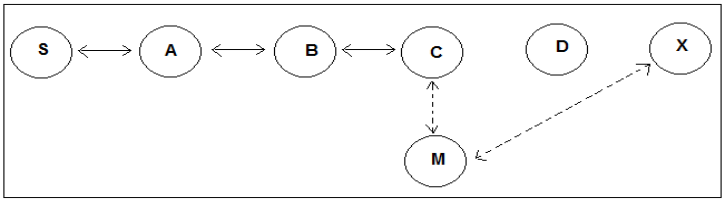


Fig.4.5 Fabrication attack example

 

**(iv) Special Attacks:**

There are also some other severe attacks in MANET network which are possible against routing protocols such as AODV and DSR.

**A. Wormhole Attack:** The wormhole attack [15] is one of the severe types of attack in which an attacker introduces two malicious nodes in the network where an attacker used to forward packets through a private "tunnel". This complete scenario described in Figure 2.9 which is given below:

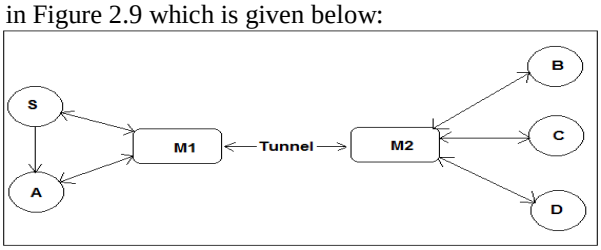


Fig. 4.6 Wormhole attack example

**B. Black hole attack:** This kind of attack is described very well in detail in [21]. In this type of attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to shares their routing tables among each other.

In the above example where there are two malicious nodes M1 and M2 which link through a private connection. In this type of attack every packet which an attacker receive from network 1 forward to other network where another malicious node exist, simple speaking these two nodes use to exchange network information and fabricate traffic among each other. The traffic between the two nodes passes through "wormhole" among each other. Due to this way it will become the cause of disrupts routing protocols and violating normal flow of routing packets. These types of attacks are very difficult to detect in a network, and become the cause of severe damages to the nodes. These types of attacks can be prevented by using mechanism packet leashes [15], which are used to authenticate nodes among each other by timing information process.

## V. RESEARCH OBJECTIVE

**The research Objective is to Analyzing the Security Issues of Routing Protocol in mobile Ad-hoc network .** This paper focuses on the two most important issues in mobile ad hoc networks – Behavior and security. Each mobile node in a MANET acts as a router by forwarding the packets in the network. Hence, one of the challenges in the design of routing protocols is that it must be tailored to suit the dynamic nature of the nodes. This chapter discusses some of the other challenges faced by the designers of routing protocols for MANETs. A complete understanding of these issues will help in designing efficient and effective routing protocols.

Some of the open challenges in designing a security solution are discussed, elucidating the practical implications with respect to confidentiality, integrity, availability and authenticity. The chapter then focuses on the network layer security and discusses secure routing in MANETs. It also classifies the attacks that are possible against the ordinary routing protocols and gives a threat assessment of the attacks. The second half of the chapter discusses another important aspect of security in MANETs – the key management issue. In particular, the chapter focuses on certificate-based authentication mechanisms. The requirements for an effective certificate-based authentication mechanism are identified, a survey of existing mechanisms is done and they are compared with respect to those requirements.

## VI. SIMULATION ANALYSIS OF MANET PROTOCOL

In this simulation we check behavior of a network using DSR, AODV, TORA protocols in scenario with 150 node, many network simulators are available to design and simulate networks in many perspectives. NS-2 (Network Simulators-2) and OPNET (Optimized Network Engineering Tools) are the two very well-known

**(i). Experimental Setup and Metrics**

For the scenario-based experiments, we used the ns-2 simulator which is available as an open source distribution [30]. Specifically, the ns-2.27 version is used on a Cygwin environment (as shown in figure 4.1). For generating the scenarios, the mobility scenario generation tool, *BonnMotion* is used. CMU's wireless extension to the ns-2 simulator is used, which is based on a two-ray ground reflection model. The radio model corresponds to the 802.11 WaveLAN, operating at a maximum air-link rate of 2 Mbps. The Media Access Control protocol used is the IEEE 802.11 Distributed Coordination Function (DCF). The traffic pattern file is generated using "cbrgen.tcl" script, which is provided along with the standard ns-2 distribution. CBR traffic with the following parameters are used for the simulations –

Table 6.1: Traffic pattern for the scenarios

| **Traffic pattern** | |
|---|---|
| Maximum number of connections | 20 |
| Application data payload size | 512 bytes |
| Packet rate | 4 packets / sec |

The metrics used for these experiments are the same as those used for evaluating the performance of AODV in a

 

battlefield scenario (section 4.4.2). In this section, the scenarios used are described.Three different scenarios were considered for the experiments in which 50 nodes are distributed over the simulation area. The scenarios depict varying node densities and link changes. They are explained in the following sections –

**Issues Faced**

This section lists some of the issues faced while running the experiments and how they were resolved.

**a. SEAD source code version compatibility**

The original SEAD source code by the authors Yih-Chun Hu, David B. Johnson, and Adrian Perrig was developed in an older version of ns-1. So the source code had to be ported to ns-2.27 since several pre-defined classes have been modified in the recent version. Hence, when the code was incorporated into the ns-2 simulator, it gave several errors during compilation. In order to resolve this, the *Active File Comparator version 1.8* was used. This software is useful in comparing two source code versions and displays the differences between them in a graphical format. A screenshot of this software is shown in figure 5.1. Using this software, the SEAD source code was compared with the latest version of DSDV (available with the ns-2 distribution). Several classes in the SEAD source code were modified to make it compatible with ns-2. The modified source code is attached in appendix-c.2.

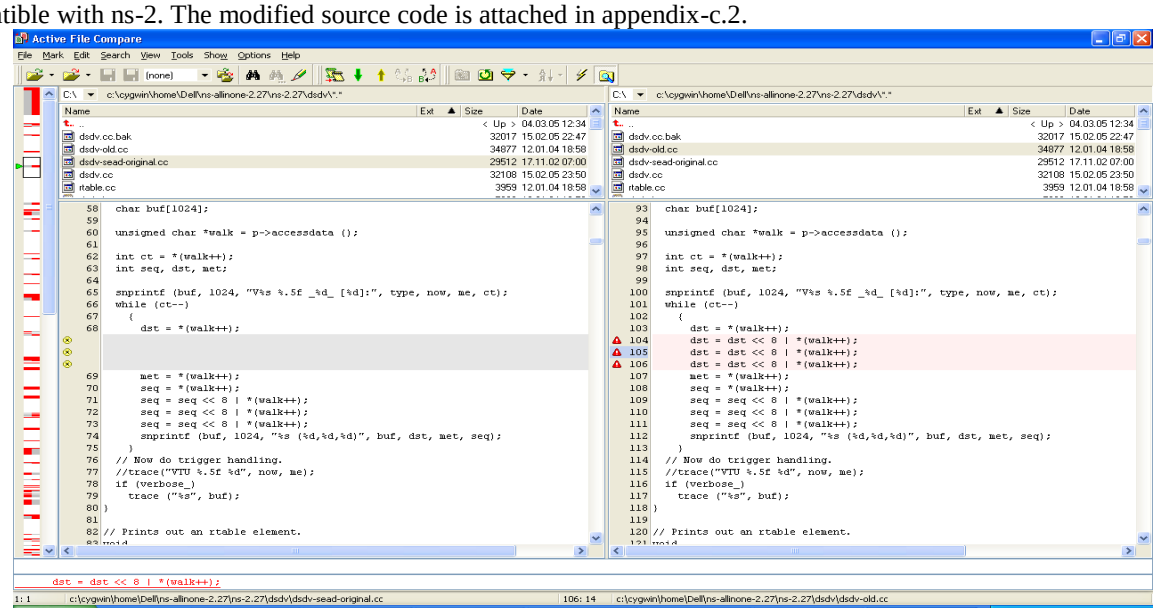


Figure 6.1: Screenshot of Active File Compare

**b. Bug in Java-based trace file Parser**

A Java program is used to trace the output files and generate the statistics such as total number of received packets at all nodes, the packet delivery fraction, the average end-to-end delay, etc. for a given scenario and a routing protocol. It generates the output as a comma separated (.csv) file which is imported into Excel spreadsheet to obtain the graphs. The new wireless trace file format can be found in the tutorial provided (Appendix-B). One of the bugs in the program was calculation of the end to end delay using the following code snippet which computes the total number of received packets and the end-to-end delay in the network –

```
                // calculate the no. of received packets and end-end delay
    if (tokens[0].equals("r") && tokens[18].equals("AGT") && tokens[34].equals("cbr"))  {
                    receives++;
                    end_time[packet_id] = time;
    }
```

Initially the condition shown in bold red, i.e. tokens [18].equals ("AGT") was omitted. This caused the program to compute *all the packets* that were of CBR type traffic. This also included the routing packets in the network. Hence the end-to-end delay obtained was much higher than the actual end-to-end delay. Once this was fixed, correct values were obtained.

**(ii) The Battlefield Scenario**

The Reference Point Group Mobility (RPGM) model is used for modeling the battlefield scenario. We define the parameters in this mobility model as shown in table 5.2 –

Table 6.2: Parameters for the battlefield scenario

| Parameters | Values |
|---|---|
| Mobility model | RPGM |
| Distribution of nodes | 10 in each group<br>5 groups |
| Simulation Area | 2000 * 2000 m |

 

| | |
|---|---|
| Probability of group change | 0.25 |
| Node speed | Max speed: 5 m/s<br>Min speed : 1 m/s |
| Maximum distance to group center | 50 m |

We consider a relatively sparsely populated set of nodes for this scenario. The total number of nodes is 50, while each node stays at a maximum of 50 meters from the group leader. We have a probability of 0.25 that there is a change in the group. For example, this may be caused due to death of a soldier or temporary movement for aiding other injured soldiers. The maximum speed of the nodes is taken as 5 m/s (which may depict military vehicles such as tanks) and minimum speed as 1 m/s (movement of soldiers).

**(ii) The Rescue Operation Scenario**

Even for this scenario, the RPGM mobility model is used. This scenario represents groups of workers operating in a relatively small area. For example, in an avalanche rescue operation we may have set of nodes communicating within a small area. We consider a relatively denser set of nodes than the battlefield scenario. The nodes have lesser probability of changing a group (0.05) as compared to the battlefield scenario. The parameters defined for this scenario are shown in table 5.3.

Table 6.3: Parameters for the rescue operation scenario

| **Parameters** | **Values** |
|---|---|
| Mobility model | RPGM |
| Distribution of nodes | 5 in each group<br>10 groups |
| Simulation Area | 1000 * 1000 m |
| Probability of group change | 0.05 |
| Maximum distance to group center | 100 m |
| Node speed | Max speed: 2 m/s<br>Min speed : 1 m/s |

**(iii) Event Coverage Scenario**

The Gauss Markov mobility model [32] was used to model the event coverage scenario. In this model we vary the degree of randomness by changing a tuning parameter. For the experiments, the speed/angle update frequency is varied to depict varying degrees of mobility within this model. The parameters are shown in table 5.4.

Table 6.4: Parameters for the event coverage scenario

| **Parameters** | **Values** |
|---|---|
| Mobility model | Gauss Markov Model |
| No. of nodes | 50 |
| Simulation Area | 500 * 500 m |
| Maximum speed of nodes | 5 m/s |
| Angle SD | 0.5 |
| Speed SD | 0.5 |

A higher density of nodes is considered for this scenario in a smaller simulation area. For example, this may depict the communication between press reporters in a large hall covering some event. The mobility of the nodes are also higher (5m/s) when compared to the rescue operation scenario. The angle and speed standard deviation are each chosen to be 0.5.

**(iv) Results**

The pause times are varied from 0 to 1000 sec for the battlefield and rescue operation scenarios. For the event coverage scenario, a parameter of the Gauss Markov mobility model called the speed or angle update frequency is varied, which is a measure of mobility. The frequency of update is varied from every 5 sec to every 60 sec. The impact of each scenario on the three metrics is studied for the three protocols chosen. The impact of each scenario on the three metrics, i.e., packet delivery fraction, end-to-end delay and the normalized routing load is studied.

**(a). Impact on the Packet Delivery Fraction (PDF)**

It is found that for the battlefield scenario, SEAD outperforms both DSDV and DSR protocols in terms of packet delivery fraction for pause times of 100-400 sec as shown in figure 5.2. This can be attributed to the fact that DSDV uses the *weighted settling delay* to reduce the number of routing table updates, which SEAD avoids. Thus SEAD typically has

 

fresher routes at a given time than DSDV, and hence the nodes have more up-to-date routing tables, implying more no. of successfully delivered packets. For higher pause times (greater than 500 sec), all the three protocols converge to give a PDF of almost 100% because the nodes are almost static and hence the congestion in the network decreases.

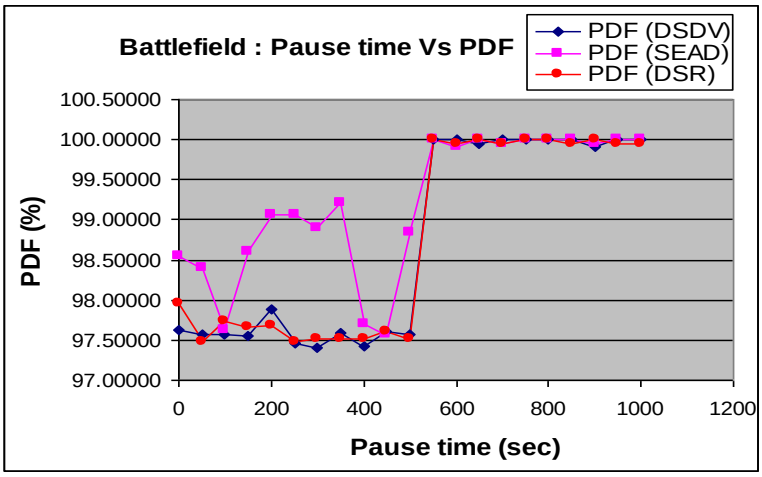


Figure 6.2: Pause time Vs PDF for battlefield scenario

.

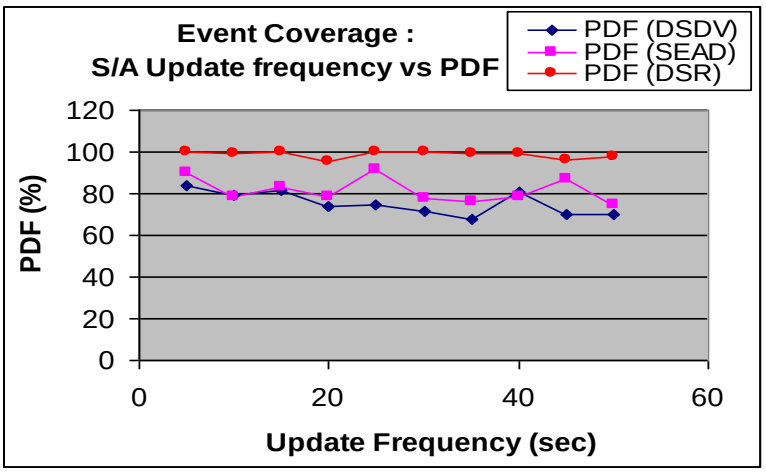


Figure 6.3: Update Frequency Vs PDF for event coverage scenario

For the event coverage scenario, the effect of varying speed/angle update frequency is shown in fig.5.3. The DSR protocol is found to have very high PDF when compared to SEAD and DSDV. This is due to the fact that DSR is a reactive protocol, and hence it adapts to changes in the network better than SEAD or DSDV, which are proactive protocols. The event coverage scenario depicts a network with denser distribution of nodes and higher mobility as compared to the battlefield scenario, which shows that SEAD adapts better to link changes and mobility in a network than DSDV

When we consider the rescue operation scenario, as shown in fig.5.4, it is found that DSR again outperforms both SEAD and DSDV and gives a PDF of almost 100% at higher pause times. On the other hand, SEAD and DSDV exhibit varied performance, with SEAD outperforming DSDV for higher pause times (greater than 700).

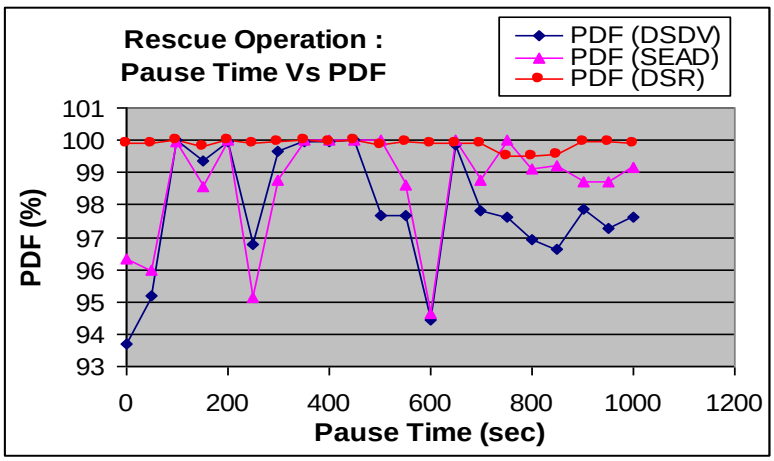


Figure 6.4: Pause time Vs PDF for rescue operation

 

**(b). Impact on the Normalized Routing Load (NRL)**

Figures 5.5, 5.6 and 5.7 show the impact of varying mobility on the Normalized Routing Load for the three scenarios. For all the scenarios, SEAD exhibits a higher routing overhead than DSR and DSDV. DSR has the least overhead of the three due to the fact that it is a reactive protocol and hence advertises routes only when required as opposed to the periodic routing updates in DSDV and SEAD.

It is found that as the density of nodes increases in the network, the Normalized Routing Load increases for DSDV and SEAD. This can be inferred from the figs. 2.a, b and c - the routing load for the event coverage scenario (high density of nodes) varies between 2 and 2.5 in fig.2.b, whereas for the battlefield scenario it varies between 0.8 and 1.2 as seen in fig.2.a. However, DSR exhibits stable values of routing loads across the three scenarios, again emphasizing the fact that a reactive routing protocol is more adaptive to the mobility of nodes than proactive routing protocol.

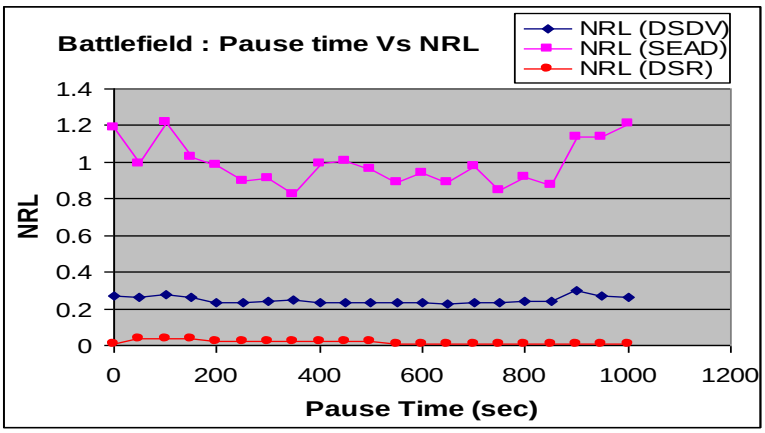


Figure 6.5: Pause time Vs NRL for battlefield scenario

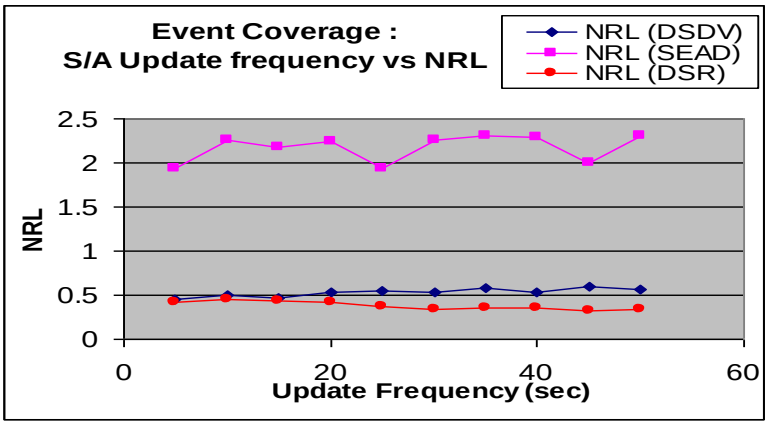


Figure 6.6: Update frequency Vs NRL for event coverage scenario

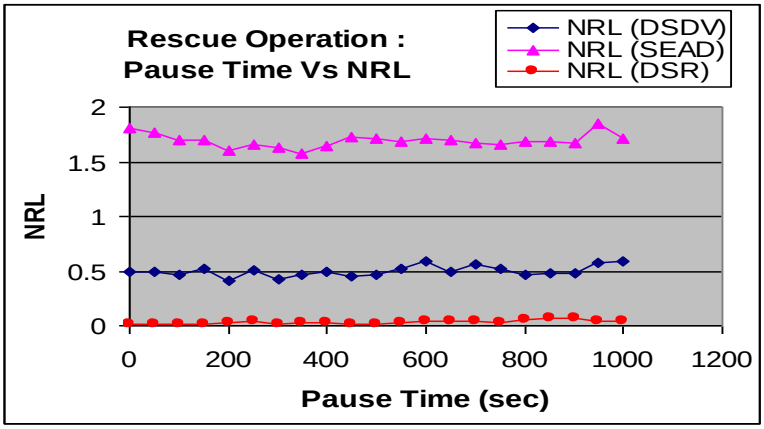


Figure 6.7: Pause time Vs NRL for rescue operation scenario

The routing load of SEAD is much higher than DSDV and DSR across all the three scenarios due to a higher number of routing advertisements sent by the nodes in the absence of the average settling delay.

**(c). Impact on the Average End-to-end Delay (AED)**

Now the impact on the most important metric, the average end to end delay is studied. As shown in figures 5.8, 5.9 and 5.10, SEAD exhibits a higher delay than DSDV and DSR. This is understandable, since the computation of hash

 

functions for authenticating the routes adds to the processing overhead at each node. Further, we find that as the mobility increases, the average end-to-end delay also increases. For a low density scenario such as the battlefield, we found that the delay is much lower for SEAD ranging between 7-8 msec (fig.5.8) as compared to a higher density scenario such as the event coverage, where it varies from 10 to 16 msec (fig.5.9).

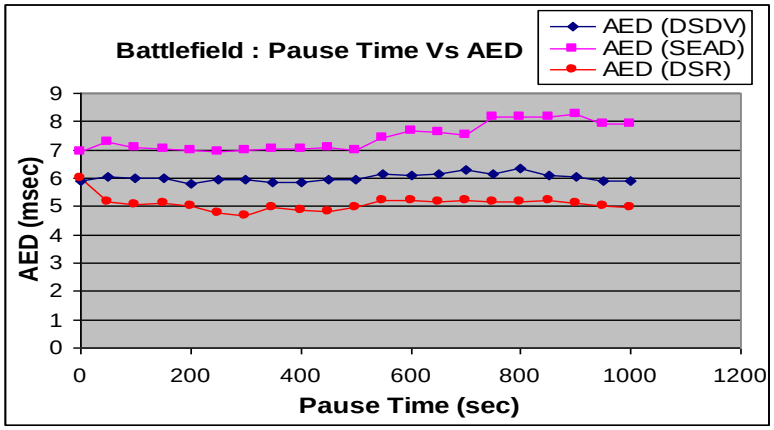


Figure 6.8: Pause Time Vs AED for battlefield scenario

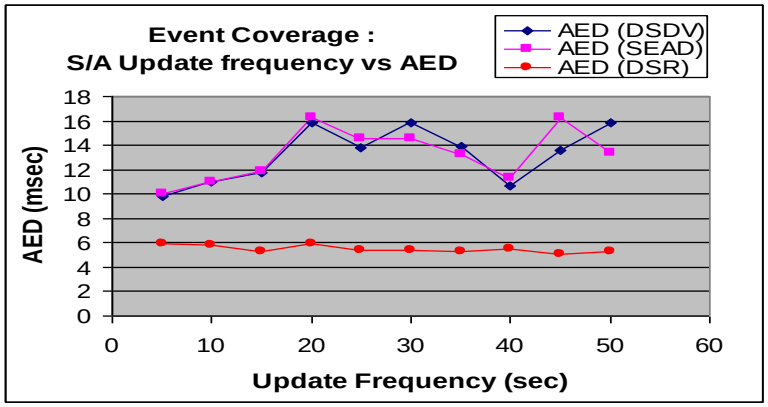


Figure 6.9: Update frequency Vs AED for event coverage scenario

DSR exhibits a lower delay than DSDV and SEAD across all the three scenarios as seen from the graphs, which bolsters the fact that a reactive protocol tends to be faster than the proactive protocols under varying loads [10]. This might be important for applications such as multimedia which require a strict upper bound on the delay. Thus, DSR will be an ideal choice for such applications when security is not an issue.

## VII. CONCLUSION

A set of scenario-based experiments were carried out to analyze the performance of the secure routing protocol, SEAD. The protocol was tested along with two other routing protocols, DSDV and DSR, representing table-driven and reactive routing protocols respectively. Some realistic scenarios are modeled using both entity and group mobility models. The performance analysis suggests that the security overhead caused by SEAD might not be suitable for applications which require a minimum upper bound on the latency. However, SEAD exhibits a higher packet delivery fraction than DSDV, indicating that it can be deployed in scenarios where delay in the network is acceptable. Some of the scenarios such as battlefield are quite demanding in terms of both throughput and security. For such scenarios, we require a combination of a reactive and proactive approach. As a continuation of this research, future work could involve the study of AODV and its secure version, the SAODV [33] which was not studied in this thesis. The simulation study of attacks in a MANET and the resulting performance degradation is also an interesting area of research. Further, the key management issue is another area which needs further research. A deeper understanding of the authentication mechanisms such as the certificate-based approach and their related performance study will be very useful in designing secure applications for MANETs.

## ACKNOWLEDGMENT

It is a great pleasure for me to express my sincere gratitude to my supervisor, **Dr. Dinesh Kumar,** Professor /Assistant Professor, Department of Computer Science & engineering of Shri Ram College of Engineering & Management, for his valuable guidance, timely advice and constant encouragement during the project work.

## REFERENCES

[1] Vijay Kumar1 and Ashwani Kush. "A New Scheme for Secured on Demand Routing" *IISTE Network and Complex Systems* ,Vol 2, No.2, 2012.ISSN 2224-610X (Paper), 2225-0603 (Online)

 

[2] Sunil Taneja & Ashwani Kush"PERFORMANCE EVALUATION OF DSR AND AODV OVER UDP AND TCP CONNECTIONS" *International Journal of Computing and Business Research (IJCBR)*, Volume 1, No. 1 December . 2010.

[3] Donatas Sumyla, Mobile Ad-hoc Networks, 03/20/2006. Available: http://ecom.umfk.maine.edu/MMobile%20Ad.pdf

[4] Kenneth Holter, "Wireless Extensions to OSPF: Implementation of the Overlapping Relays Proposal",Master thesis,Department of Informatics, University of Oslo,Norway, 2nd May

[5] S. Corson & J. Macker"Mobile Ad hoc Networking:Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, Oct. 1999. Available: http://tools.ietf.org/html/rfc2501

[6] David B. Johnson,David A. Maltz & Josh Broch"DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks" Computer Science Department Carnegie Mellon University Pittsburgh, PA 15213-3891Available:http://www.monarch.cs.rice.edu/monarch-papers/dsr-chapter00.pdf [7] Kenneth Holter" *Comparing AODV and OLSR*" 23rd April 2005. Available:http://folk.uio.no/kenneho/studies/essay.pdf

[8] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003 Available: http://www.ietf.org/rfc/rfc3626.txt.

[9] P. Jacquet,P. Muhlethaler,T. Clausen,A. Laouiti,A. Qayyum,L. Viennot"Optimized link state routing protocol for ad-hoc networks" in International Multi Topic Conference 2001(IEEE),Dec. 2001. Available:http://menetou.inria.fr/~muhletha/olsr.pdf

[10] Amandeep Makkar, Bharat Bhushan, Shelja, and Sunil Taneja"Behavioral Study of MANET Routing Protocols" *International Journal of Innovation, Management and Technology*, Vol. 2, No. 3, June 2011. Available: http://www.ijimt.org/papers/133- M548.pdf

[11] David B Johnson and David A Maltz. "*Dynamic source routing in ad hoc wireless networks"*. In Imielinski and Korth, editors, Mobile Computing, volume 353. Kluwer Academic Publishers, 1996.

[12] Haas Z.J, " *A new routing protocol for the reconfigurable wireless network"*. In Proceedings of the 1997 IEEE 6th International Conference on Universal Personal Communications, ICUPC '97, San Diego, CA, October 1997; pp.562--566.http://www.ics.uci.edu/~atm/adhoc/paper-collection/haas-routing-protocol-icupc97.ps.gz

[13] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and Elizabeth M. Belding royer. *"A Secure Routing Protocol for Ad Hoc Networks" (ARAN)* In International Conference on Network Protocols (ICNP), Paris, France,November,2002. www.cs.ucsb.edu/~kimaya/icnp2002.pdf

[14] Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, "*Mobile Ad Hoc Networking*", ISBN: 0-471-37313-3, Wiley-IEEE Press: *Chapter 12: Ad hoc networks Security* Pietro Michiardi, Refik Molva http://www.eurecom.fr/~michiard/pub/michiardi-adhoc.pdf

[15] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "*Routing Security in Wireless Ad Hoc Network*," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[16] Yih-Chun Hu, David B. Johnson, Adrian Perrig. *"SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks"*, Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp: 3-13,Jun2002. http://www.cs.colorado.edu/~rhan/CSCI_7143_001_Fall_2002/Papers/Perrig2002_wmcsa02.pdf

[17] Yih-Chun Hu, Adrian Perrig, David B. Johnson. *"Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks"* MobiCom 2002, September 23-28, 2002, Atlanta, Georgia,USA. http://lambda.cs.yale.edu/cs425/doc/ariadne.pdf

[18] A. Perrig, R. Canetti, D. Tygar, and D. Song, "*The TESLA Broadcast Authentication Protocol*," Cryptobytes,, Volume 5, No. 2 (RSA Laboratories, Summer/Fall 2002), pp. 2-13.http://www.rsasecurity.com/rsalabs/cryptobytes/

[19] P. Papadimitratos and Z. Haas. *"Secure routing for mobile ad hoc networks" (SRP)* SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, pp. 27--31, January 2002. http://wnl.ece.cornell.edu/Publications/cnds02.pdf

[20] S.M Mousavi et al, ´´Mobile Ad HOC Networks with Model Based Adaptive Mobility Prediction,´´ *IEEE Int'l.Conf.on Wireless Computing, Networking and Communications' (Wimob2007).*

[21] S.Jardosh, P.Ranjan ''A survey: Topology Control for Wireless *Networks'' IEEE International Conference on Signal Processing, Communications and Networking, Madras Institute of Technology, India, Jan 4-6. 2008. pp422-427.*

[22] A. Pathan, et al. ´Security In Wireless Sensor Networks: Issues and Challenges'' *Proc. of the IEEE ICACT, Vol.2 pp1043-1048, March, 2006.*

[23] R.Molva, P.Michiardi ''Security in Ad Hoc Networks'' *Proceedings of the Personal Wireless Communications (PWC2003), Venice Italy, Sept.2003*

[24] B.Wu et al ''Secure and Efficient Key Management in Mobile Ad Hoc Networks'' *Journal of Computer Applications archive Vol.30, No.3, pp937-954, 2007.*

[25] B.Wu et al.´´Secure and Efficient key Management in Mobile Ad Hoc Networks, ´´ *Proc.of the 19th IEEE Int'l. Workshop on Parallel and Distributed Processing Symposium (IPDPS'05) Vo.18, pp288.1, 2005*

 