A SIMULATION AND ANALYSIS OF SECURED AODV PROTOCOL IN MOBILE AD HOC NETWORKS

Sesha Bhargavi Velagaleti[1], M. Seetha[2], S. Viswanadha Raju[3]

[1]Assistant Professor, IT Department, [2]Professor, CSE Department, GNITS, Shaikpet, Hyderabad, India
[3]Professor, CSE Department, JNTUK, Hyderabad, India
b.velagaleti@gmail.com, smaddala2000@yahoo.com, viswanadha_raju2004@yahoo.co.in

Abstract

A Mobile ad hoc Network is a wireless network, which is dynamic in nature, that can be simulated by infra structure less connections in which every node itself can act as a router. There are many significant routing protocols proposed for providing significant benefits in terms of performance, reliability, security and many other issues also have been addressed. An efficient way of evaluating the performance of MANETS is to simulate them. Of the many simulators available, Ns-2 has gained increasing popularity because of its many efficient features. The main aim of this simulator is to provide better networking environment for research and educational purposes. In this paper, we try to propose a new routing protocol and tried to implement it on NS-2 . We also tried to compare the results with other protocols.

Keywords: *MANET, AODV, Network Simulator, DSR*

----------***----------

1. INTRODUCTION

MANETS provide more flexibility in the creation of a network in situations like where there is no possibility or less possibility in setting up the predefined infrastructure. Unlike a node in an infrastructure based network, all the nodes in a MANET cooperate with each other to perform routing. All the nodes in a network are very free to move and hence change the links very easily. Because the radio transmission range is very less, there is a lot of overhead involved with respect to routing, security in particular. This is because the nodes are more prone to failures and compromises in ad hoc networks because of their mobility.

MANET is a wireless ad-hoc network which is also a self-configuring network of mobile routers (and associated hosts) that are connected by wireless links, and all these together form an arbitrary topology. The nodes are free to move randomly and manage themselves and also perform the task of routing as the nodes themselves act as routers. So the network's topology changes very rapidly and unpredictably. This type of network can easily act as a standalone network as well as has the capability to connect to the internet. With this feature, MANET s can be widely used for commercial purposes very easily. MANET s are very self-organizing and adaptive. Networks are formed on the fly and devices can leave and join the network at any time.

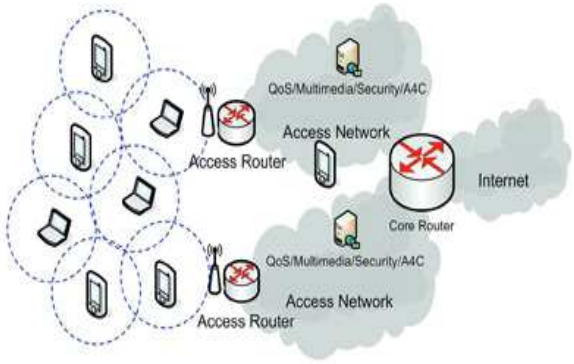


Fig1: A Mobile Ad hoc Network

The communication between the devices in this wireless network which are in their radio range will be in a peer-peer fashion. Intermediate devices can be used if the devices wish to communicate with those that are out of the radio range. Every device acts as a host when providing any information or requesting from /to any other node in the network. These devices acts as routers while discovering and maintaining routes for other nodes in the network.

Mobile ad hoc networks became a popular for research as laptops and 802.11/Wi-Fi wireless networking became widespread from 1990s. Many researchers are evaluating the protocols with different degrees of mobility within a bounded space, usually with all nodes within a few hops of each other, and usually with nodes sending data at a constant rate. The

packet drop rate, the overhead introduced by the routing protocol, and other measures are also evaluated for different protocols.

1.1 Characteristics of Mobile Ad Hoc Networks

1. MANETs doesn't depend on any fixed infrastructure for the operation of mobile nodes.
2. Any node or device can freely join and leave the network at any time , which accounts
3. They can be easily attached to any internet or cellular networks as they need not operate in standalone mode only.
4. It can be rapidly deployed with user intervention.
5. In MANET, each node act as both host and router. That is it is autonomous in behaviour.
6. Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
7. Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
8. Mobile nodes are characterized with less memory, power and light weight features.
9. The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
10. Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
11. All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
12. High user density and large level of user mobility.
13. Nodal connectivity is intermittent.

1.2 MANET Challenges

A MANET environment has to overcome certain issues of limitation and inefficiency. It includes:

- The wireless link characteristics are time-varying in nature: There are transmission impediments like fading, path loss, blockage and interference that adds to the susceptible behaviour of wireless channels. The reliability of wireless transmission is resisted by different factors.
- Limited range of wireless transmission – The limited radio band results in reduced data rates compared to the wireless networks. Hence optimal usage of bandwidth is necessary by keeping low overhead as possible.
- Packet losses due to errors in transmission – MANETs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues (high bit error rate (BER)), interference, frequent breakage in paths caused by mobility of nodes, increased collisions due to the presence of hidden terminals and uni-directional links.
- Route changes due to mobility- The dynamic nature of network topology results in frequent path breaks.
- Frequent network partitions- The random movement of nodes often leads to partition of the network. This mostly affects the intermediate nodes.

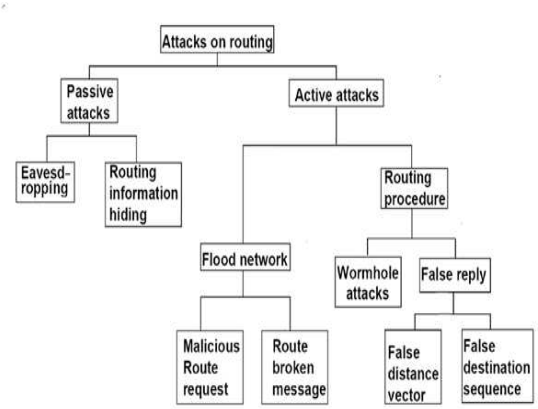


Fig2: Types of Attacks on MANET's

The application of this wireless network is limited due to the mobile and ad hoc nature. Similarly, the lack of a centralized operation prevents the use of firewall in MANETs. It also faces a multitude of security threats just like wired networks. It includes spoofing, passive eavesdropping, denial of service and many others. The attacks are usually classified on the basis of employed techniques and the consequences.

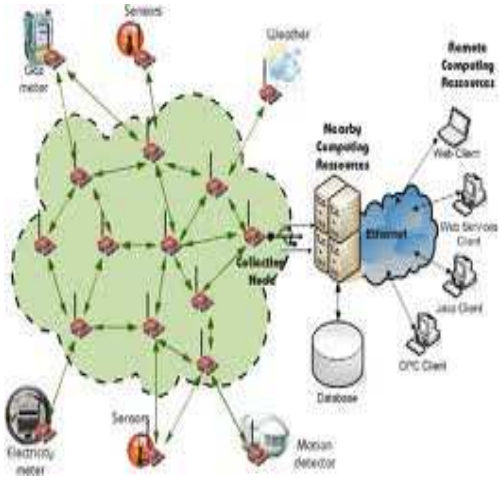


Fig3: Architecture of MANET

1.3 Applications of MANET's

With the increase of portable devices as well as progress in wireless communication, ad-hoc networking is gaining importance with the increasing number of widespread applications. Ad-hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use.Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infra structured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include:

1. **Military Battlefield:** Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.
2. **Commercial Sector:** Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small hand held. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.
3. **Local Level:** Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.
4. **Personal Area Network (PAN):** Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context.8.5 MANET-VoVoN: A MANET enabled version of JXTA peer-to-peer, modular, open platform is used to support user location and audio streaming over the JXTA virtual overlay network. Using MANET-JXTA, a client can search asynchronously for a user and a call setup until a path is available to reach the user. The application uses a private signalling protocol based on the exchange of XML messages over MANET-JXTA communication channels.

1.4 Limitations of MANET's

1. Most of the nodes constantly change their positions in the network which makes routing discovery very complex.
2. Out-of date routes are also generated in the network, which adds more overhead.
3. Most of the links are asymmetric in ad hoc networks.
4. As links come and go depending on their transmission characteristics,one transmission may interfere with other, which causes lot of interruptions in the entire network.
5. Because of the dynamic topology, the medium characteristics also change frequently, and more complex routing algorithms have to be employed.

1.5 Routing protocols for MANET's

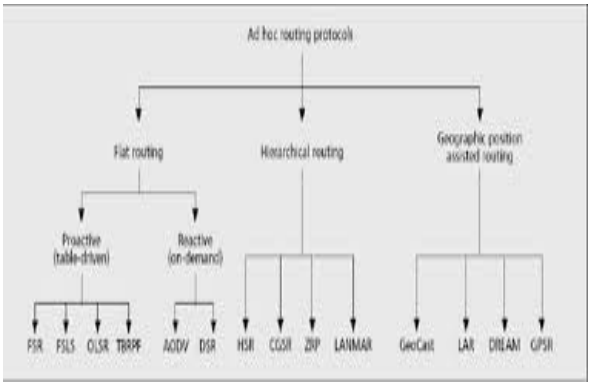


Fig4: Classification of Routing Protocols

There are many ways of classifying the routing protocols but most of them rely on routing strategy and network structure. Mainly these are classified as Flat, hierarchical, and Geographic position based routing protocols. Another major classification is based on whether they are on-demand or table-driven. Flat routing protocols are further divided into several types based on whether the routing table is generated statically before itself or whether it is generated only ion demand as when the need comes so as to make a routing decision. Examples of table-driven protocols are

a) Optimized Link state Routing (OLSR)
b) Fish-eye state routing (FSR)
c) Destination -Sequenced Distance Vector Routing (DSDV)

d) Cluster-head Gateway Switch Routing Protocol (CGSR)

Examples of on-demand routing protocols are:
a)Ad-hoc on demand Distance Vector(AODV)
b) Dynamic source Routing Protocol (DSR)
c) Temporally ordered Routing Algorithm (TORA)
d) Associativity based routing (ABR)
e) Signal Stability based Associative Routing (SSAR)
f) Location –Aided Routing Protocol (LAR)

Several hybrid protocols are also used to find a balance between the above two types which take the domain information into account. Examples of hybrid routing protocols are Zone routing protocol and Wireless ad hoc routing protocol. As the size of the network increases, flat routing protocols does not perform well because of the lot of overhead incurred . In such cases hierarchal routing algorithms perform better. Examples of such algorithms are
a) Hierarchical state routing
b) Zone routing protocol
c) Cluster head Gateway switch routing protocol
d) Landmark ad hoc routing protocol

Another class of routing protocols are based on te location information and takes the geographic co-ordinates into account and maintain reference points to compute the routes. Examples of such algorithms are Geocast (geographic addressing and routing), DREAM (Distance Routing effect algorithm for mobility) and GPSR (Greedy perimeter stateless routing).

2. EXISTING WORK

The secure routing algorithms in wireless communication are addressed and have been suggested for increasing the security levels [4]. However, these algorithms are unable to protect the network from attackers, who acquired the key information [5]. J.Li et al[6] proposed a common key encryption mechanism for MANETs using Dynamic Source Routing(DSR). Drawback of this model is that it dropped more packets even if the network had few malicious users [7]. Adhoc On-Demand Distance Vector (AODV), which is used to provide secure and reliable data transmission over the MANETs [8]. Several strategies are used to detect the non-cooperate nodes while forwarding the data packets to the destination [9]. In [10], authors discussed a trusted approach to establish the communication between the mobile users. Here, the communication takes place based on the watch dog. The trusted values are represented from -1 to +1. A black hole attack is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination[11]. Smith et al[12] examined the routing security of distance vector protocols in general and developed countermeasures for vulnerabilities by protecting both routing messages and routing updates. They propose sequence numbers and digital signatures for routing messages and updates as well as including predecessor information in routing updates.

3. IMPLEMENTATION OF MANET ROUTING PROTOCOL ON NS2

3.1 Introduction to NS2

NS2 is available under Linux, with a GPL license. Few algorithms like DSR, AODV and DSDV were already implemented on this simulator.NS2 is a network simulator; built with C++ and TCL. The main goal here is to simulate different kinds of networks, and to implement and test different routing algorithms on those networks, and to find the limitations of each. It has been developed in the California University, by LBL, Xerox PARC, UCB, and USC/ISI through the VINT project supported by DARPA. NS2 was initially built for fixed wired networks. First, this simulator was build for fixed network: all links among nodes were wired. That means that the neighbour had no direct neighbour: if two nodes were very close, they don't communicate each other if they don't have a cable between each other. So, later, an extension for wireless network was developed by UCB Deedless, CMU Monarch projects and Sun Microsystems.

The simulator is composed of two parts: 1. The TCL code: it is used to communicate with the simulator, and permits to define different simulation parameters.

3.2 AODV: Ad-hoc On Demand Distance Vector

AODV is a distance vector type routing. The basic feature of AODV is that the active nodes need not maintain the routes to destinations. AODV works well when the communication end points have correct routes to the router. Different messages used by the AODV protocol for routing management are : Route Requests(RREQs), Route Replies(RREPs), and Route Errors(RERRs).UDP is used to receive messages and some sort of IP header processing is also applied. It makes use of a destination sequence number for each route entry. The destination sequence number is created by the destination for any information it sends to request nodes. These are used to know which new routes are found on the way, of the many routes available. A route with the highest sequence number is chosen from multiple routes available for the node. An RREQ is broadcasted as and when there is a need to find a route to another node, until either the destination is reached or another node is found with a fresh enough route to the destination (a fresh enough route is a valid route entry for destination whose associated sequence number is at least as great as that contained in the RREQs). Then a RREQ is sent back to the source and the discovered route is made available. Acitive nodes which are part of the connection mar send HELLO messages to its immediate neighbours. If Hello messages stop arriving from a neighbour beyond some given time threshold,

the connection is assumed to be lost. When a node detects that a route to a neighbour node is not valid it removes the routing entry and send a REER message to neighbours that are active and use the route; this is possible by maintaining active neighbour lists. This procedure is repeated at nodes that receive REER messages. A source that receives an REER can reinitiate a RREQ message. The main drawback of this AODV is that there is no provision to handle unidirectional links.

3.3 Dynamic Source Routing Protocol

Dynamic Source Routing (DSR) is routing protocol for wireless mesh networks. Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).

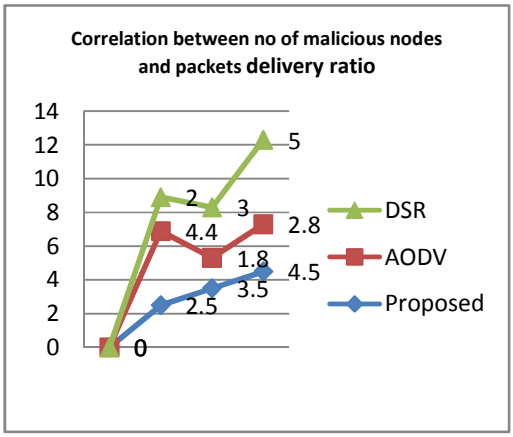
To return the Route Reply, the destination node must have a route to the source node. If the route is in the Destination Node's route cache, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Request message header (this requires that all links are symmetric). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The erroneous hop will be removed from the node's route cache; all routes containing the hop are truncated at that point. Again, the Route Discovery Phase is initiated to determine the most viable route.

3.4 Simulation Parameters

Simulation time	3000s
No.of clusters	12
Transmission range	200m
No.of cluster heads	10
No. of nodes	100
Topology size	1000*1000m
Routing protocol	AODV
Node mobility	0 to 10m/s
Channel capacity	2Mbps
Traffic type	CBR
CBR packet size	512 bytes
Frequency	2.4GHz
Simulator	NS2
Pause time	1s
Number of packets	30000
Mobility model	Random way

3.5 Simulation Results

We tried to implement this model with 250 nodes with different arrival rates and with 3 clusters heads. The simulation results are shown in the below figure. No. of data packets sent are around 5 to 20 packets/second. We tried to compare the no. of malicious nodes with the packet delivery ratio so that the performance of the network in case of huge no. of malicious nodes can be observed so as to take any preventive action. From the obtained results we observed that the proposed model delivered around 70% of the packets when compared to the existing AODV protocol which delivers almost 62% of the packets. The total network load is also compared with end-to-end delay and was found that as the network load increased the delay also gradually increased. We can also conclude that AODV transferred packets at a lesser delay compared to other protocols.



CONCLUSIONS AND FUTURE SCOPE

In this paper, we tried to implement several routing protocols like AODV and DSR for MANET's and compared the results obtained with our proposed protocol with different no of malicious nodes to identify the performance of the network under different scenarios. The simulation results were shown and it is found that AODV delivers packets with lesser delays when compared to DSR protocol. In future, extensive complex simulations could be carried out for different parameters with more increased no. of nodes and more detailed in-depth analysis of the entire network under various scenarios can be done.

REFERENCES

[1]. TCP over Ad Hoc Networks: NS-2 Simulation Analysis by Ren Mao, Haobing Wang, Li Li, Fei Ye
[2]. SIMULATION AND COMPARISION OF AODV AND DSR ROUITNG PROTOOCLS IN MANETS by vivek kumar under the supervision of M.sumit miglani.
[3]. NEW SECURITY ALGORITHM FOR MOBILE ADHOC NETWORKS USING ZONAL ROUTING PROTOCOL by G.Varaprasad, S. Dhanalakshmi,, M. Rajaram ,Department of Computer Science and Engineering, B.M.S. College of Engineering, Bangalore, India
[4]. Y.Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", ACM Wireless Networks, Vol. 9, pp. 545 – 556(2003).
[5].Y. C. Hu and A. Perrig, "A Survey of Secure Wireless Adhoc Routing," IEEE Security and Privacy Magazine, Vol. 2, No. 3, pp. 28-39(2004).
[6].J. Li, J. Jannotti, Douglas S. J. D. Couto, David. R. Karger, and R. Morris, "A Scalable Location Service for Geographic Adhoc Routing", In Proceedings of International Conference on Mobile Computing and Networking, pp. 120-130(2002)
[7]. B. Karp and H. Kung, "Greedy Perimeter Stateless Routing for Wireless Networks", In Proceedings of International Conference on Mobile Computing and Networking, pp. 243-254(2003).
[8].Y. A. Huang and W. Lee, "Attack Analysis and Detection for Adhoc Routing Protocols," In Proceedings of International Symposium on Recent Advances in Intrusion Detection, pp. 125-145(2004).
[9]. L. Zhou S. B. Fred, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority", ACM Trans. on Computer Systems, Vol. 20, No. 4, pp. 329-368(2002).
[10]. M. Gasser and E. McDermott, "An Architecture for Practical Delegation in a Distributed System", In Proceedings of IEEE Symposium on Security and Privacy, pp. 20-30(2004).
[11]. 11. Z. J. Haas, M. Perlman, "The Performance of Query Control Schemes of Zonal Routing Protocol", IEEE Trans. on Networking, vol. 9, no. 4, pp. 427-438(2001).
[12]. Bradley R. Smith, Shree Murthy, and J.J. Garcia-Luna-Aceves, "Securing Distance Vector Routing Protocols", In Proceedings of Internet Society Symposium on Network and Distributed System Security, pp. 85-92(1997).
[13]. "Simulation Study and Implementation on Routing Protocols in MANET" IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012 ISSN (Online): 2231 –5268 Anju Yadav M.Tech Scholar, Shekhawati Engineering College, Jhunjhunu, Rajasthan.
[14].Wikipedia for AODV and DSR Routing Protocols.