A Simulation and analysis of Secured S-DSR Protocol in Mobile ad hoc Networks

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

Assistant Professor , IT Departmnet, GNITS, Shaikpet, Hyderabad, India.
Professor, CSE Department, GNITS, Shaikpet , Hyderabad, India
Professor, CSE Department, SIT,JNTUH, Hyderabad, India.

Abstract

A MANET is a special kind of wireless network, which can be treated as a collection of mobile nodes co-existing with each other without the need of any fixed infrastructure. Because of the limited physical security, ad hoc topology, battery-based operation, and lack of a centralized coordinator, it is more prone to attacks than a wired network .Our main aim is to provide secure data transmission between the source and destination nodes. The simulation is carried out for different number of mobile nodes using network simulator with the help of 1000 mobile nodes. We have compared this S-DSR model with the existing models such as DSR and AODV. This model has shown the better results in terms of packet delivery, packet drop, and delay even in the presence of more no.of malicious nodes.

Keywords: MANET, Network Simulator, DSR, AODV

1. INTRODUCTION

Mobile Ad hoc Network (MANET) has attracted a large community of users due to its self-design, self-maintenance,
and cooperative environments. The main goal of MANETS is to enhance mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes themselves form the network routing infrastructure in an ad hoc fashion. 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. In MANET, all the nodes are mobile with dynamic topology, i.e., the nodes will move in and out of the network as and when required. The basic structure of the MANET is shown in Figure 1. Here, the mobile devices such as PDAs and laptops are connected using the WLAN and are used to route the data packets. In MANET, all the nodes are actively discovered the topology and the data are forwarded to the destination through multiple-hops. It uses the wireless channel and asynchronous datatransfer mechanism through these multiple hops. Less configuration, no need of a centralized authority and fast deployment features make MANETS most suitable for emergency situations like natural calamities, emergency medical situations, military applications etc., Unlike a node in an infrastructure based network, all the nodes in a MANET cooperate with each other to perform routing. 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. Vital characteristics of MANET's include dynamic topology without the use of fixed infrastructure, deployment, no user intervention, and autonomous behavior etc. Mobile Ad-hoc Networks (MANETs) are future wireless networks consisting entirely of mobile nodes that communicate on-the-move without base stations. Nodes in these networks will both generate user and application traffic and carry out network control and routing protocols. Rapidly changing connectivity, network partitions, higher error rates, collision interference, and bandwidth and power constraints together pose new problems in network control—particularly in the design of higher level protocols such as routing and in implementing applications with Quality of Service requirements.

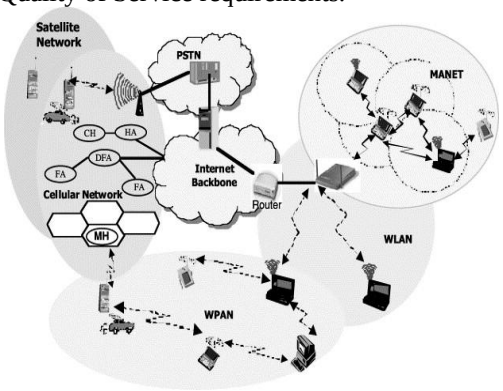


Fig1: Architecture of MANET

1.2 MANET Challenges

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

- Time Varying nature of the wireless links.
- Multipath Fading
- Path loss and interferences
- Limited range Connectivity
- Less coverage area for wireless transmission
- Huge susceptability to packet losses due to transmission errors.
- Dynamic Routing updates
- Presence of hidden terminals
- More frequent network changes
- Adhoc nature of the network
- Security threats like DOS, eavesdropping,spoofing etc.,

2. RELATED WORK

As a promising network type for future mobile application, MANETs are attracting more and more researchers. Mobile ad hoc networks are resource constrained and hence Routing in mobile ad hoc networks is more challenging task. Many researchers have done work on analyzing the characteristics of different routing protocols in mobile ad hoc networks. Rachit Jain, Laxmi Shrivastava [1] analyzed the performance of AODV & DSR on the basis of Path Loss Propagation models based on various performance metrics in order to create a substantial understanding of choosing the correct protocol for any active operating environment. Dhananjay Bisen et al. [2] studied the effect of pause time on AODV, DSR and DYMO routing protocols in mobile ad hoc networks based on parameters like Packet Drop Ratio (PDR), Throughput, Jitter and End to End Delay with variations in Pause Time of network. They concluded that DSR performs better than AODV and DYMO under different situations with variation in pause time and performance of DYMO is better than DSR in some situations. Monika at el. [3] compared AODV, DSDV and DSR Routing Protocols in Vehicular Network Using EstiNet Simulator based on parameters like throughput, number of packets dropped. The performance of AODV found to be better in most situations. M.L Sharma et al. [4] analyzed the performance of MANET routing protocols under CBR and FTP traffic classes under different network scenarios like pause time, offered load (i.e. number of source destination pairs), node speed. The results shows that for CBR traffic, AODV performs better than DSR and WRP in terms of Packet Delivery Ratio(PDR), Throughput and routing overhead and for FTP traffic, DSR performs better than AODV and WRP in terms of packet delivery ratio and throughput. Liang Qin, Thomas Kunz [5] provides a method to increase the packet delivery ratio in DSR by link protection through link breakage prediction algorithm. They also proposed that enhanced route cache maintenance based on the link status can further reduce the number of dropped packets.

3. ROUTING PROTOCOLS FOR MANET'S

One of the important challenges with MANET's is forwarding of packets from source to the destination node. To perform this routing process, many algorithms were proposed to effectively find the effective path from source node to the destination node.Several criteria like the topology of the network, the link cost metrics used in the network, geographical position of the nodes in the network, availability of resources, topology updates etc., were considered to further classify these routing protocols proposed.

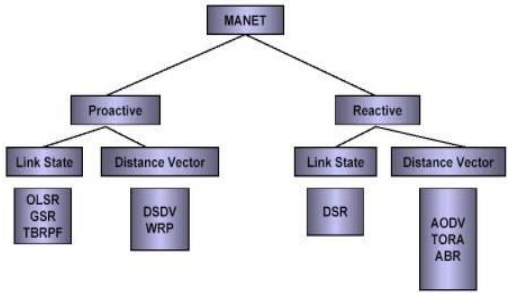


Fig2: Classification of Routing Protocols

The majority classification of routing protocols is mainly based on how the topological updates are informed to the nodes in the network. Entire set of routing protocols were mainly classified as either proactive or reactive. If the routing updates are done statically, they are called as proactive routing protocols, which doesn't consider any changes in the topology of the network once route discovery is completed. The other class of protocols are the reactive protocols which updates the routing information dynamically, as and when the topology of the network changes. Examples of proactive protocols are OLSR, WRP, GSR etc. Examples of proactive protocols are TORA, DSR, DSDV, ODMRP etc.

4. SECURED DYNAMIC SOURCE ROUTING (S-DSR)

In this protocol, concept of source routing is used in which a route is created only when it is required by the source. This protocol is mainly based on the concept of link state routing algorithm, which is an on-demand routing protocol. The main advantage with this protocol is that the routing overhead is very less compared to the other protocols.

This protocol mainly works in two phases:1.Route Discovery 2.Route Maintenance. In Route Discovery,when a source node S wants to send a packet to the destination D, it first checks its route cache. If there is an entry for the destination node, then the source uses the available route in cache. If route not found or the the route cache has an expired route, then it initiate the route discovery process. Route cache contains the recently discovered routes. Route discovery requires 7 fields during this process such as source id, destid, ReqID, Address list, Hop limit, Network Interface List, Acknowledgment list. Then source node broadcasts the message to its neighbours. Moreover, source node also maintains a replica of messages sent in its send buffer. Packets can be dropped if send buffer is full or the time limit for route discovery is over. When a nodes destination or the intermediate node having route to

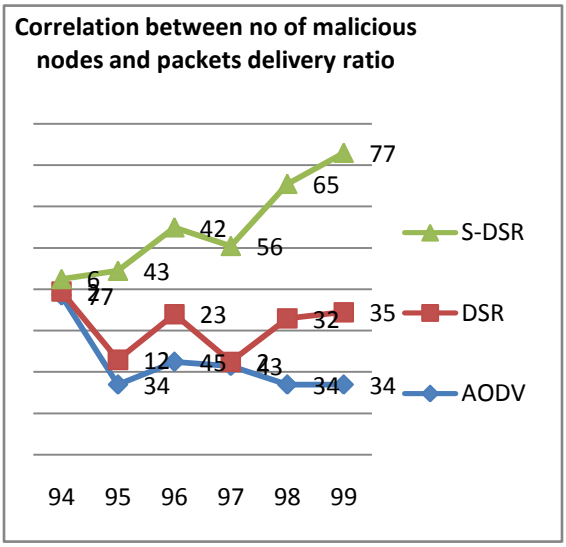
destination receives the route request message, it generates route reply. Route maintenance includes monitoring the routes against failure through route error messages and route cache. There is no need of keeping routing table in S-DSR protocol. Route cache can further decrease route discovery overhead. S-DSR reduces overhead of route maintenance. However S-DSR is not scalable to large networks and packet Size grows with length of the route due to source routing.

5. SIMULATION ENVIRONMENT

Simulator	NS-2.34
Simulation Area	1000m X 1000m
Mobile Nodes	10,20,50,75
Pause Time	100,200,300,400,500 Sec
Speed	2,3,5,7,10 m/s
Channel	Wireless
Routing Protocols	AODV & DSR
Traffic Sources	UDP
No. of connections per Sec	1.0,2.0,3.0,4.0,5.0
Simulation Time	500 Sec.

6. SIMULATION RESULTS

DSR protocol was developed based on the functionality of RIP protocol, and is mainly developed for ad hoc networks. Routing tables stored at each node are used to discover the route .Maintaining and managing these routing tables forms the main complexity of this routing protocol. It has been observed that our proposed protocol works with more lesser delays and hence more packet delivery ratios under different no.of malicious nodes.



7. CONCLUSION AND FUTURE SCOPE

In this paper, implemented the routing protocol DSR for MANET's has been implemented and the results obtained were compared 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 the proposed protocol delivers packets with lesser delays when compared to DSR protocol. In future, more complex simulations could be carried out for different parameters and more detailed in-depth analysis of the entire network under various scenarios can be done. In DSR, nodes has to periodically transmit the routing table updates, regardless of network traffic. These update packets are broadcast throughout the network so every node in the network knows how to reach every other node. As the number of nodes in the network grows, the size of the routing tables and the bandwidth required to update them also grows. As the topology changes dynamically, DSR is unstable until update packets propagate throughout the network.

8. REFERENCES

[1] Rachit Jain1, Laxmi Shrivastava "Study and Performance Comparison of AODV & DSR on the basis of Path Loss Propagation Models" International Journal of Advanced Science and Technology Vol. 32, July, 2011

[2] Dhananjay Bisen at el. "Effect of Pause Time on DSR, AODV and DYMO Routing Protocols in MANET" Manuscript received November 20, 2009.

[3] Monika at el. "Comparative Study of AODV, DSDV and DSR Routing Protocols in Vehicular Network Using EstiNet Simulator" International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012

[4] M.L Sharma at el." Performance Evaluation of MANET Routing Protocols under CBR and FTP traffic classes" Int. J. Comp. Tech. Appl., Vol 2 (3), 392-400 ISSN: 2229-6093

[5] Liang Qin Thomas Kunz "Increasing Packet Delivery Ratio in DSR by Link Prediction" Proceedings of the 36th Hawaii International Conference on System Sciences - 2003

[6] International Journal of Advanced Research in Computer Science and Software Engineering Research Paper "A Comparative Study of AODV & DSR Routing Protocols in Mobile Ad-Hoc Networks "Anit Kumar* M.Tech., Department of Computer Science and Applications, KurukshetraUniversity, Kurukshetra, Haryana, India.

[7] TCP over Ad Hoc Networks : NS-2 Simulation Analysis by Ren Mao, Haobing Wang, Li Li, Fei Ye

[8] SIMULATION AND COMPARISION OF AODV AND DSR ROUITNG PROTOOCLS IN MANETS by vivek kumar under the supervision of M.sumit miglani.

[9] 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

[10] Y.Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", ACM Wireless Networks, Vol. 9, pp. 545 – 556(2003).

[11] 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).

[12] 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).

[13] 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).

[14] 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).hekhawati Engineering College, Jhunjhunu, Rajasthan.

[15] Wikipedia for AODV and DSR Routing Protocols.

[16] Routing in Ad Hoc Networks of Mobile Hosts,Dr. Gerard McLeanB. Cameron Lesiuk December 2, 1998Department of Mechanical Engineering,University of Victoria, Victoria, BC, Canada