International Journal of Engineering Research & Management Technology ISSN: 2348-4039
May-2015 Volume 2, Issue-3
Email: editor@ijermt.org www.ijermt.org

Securing Dynamic Source Routing over Mobile Ad-Hoc Network using NS2

Nidhi Bansal
M.Tech Scholar, CSE Dept
HEC, Kurukshetra University
Haryana, India

Ms. Monika Mehla
Assistant Professor, CSE Dept
HEC, Kurukshetra University
Haryana, India

ABSTRACT:
Mobile Ad Hoc networks (MANET) are composed of a group of wireless mobile nodes that can communicate with each other. Different from normal networks, MANET is easy to be attacked. The attacking to the protocol can paralyze the network, so the security of routing protocol is an important part of the Ad Hoc networks security. We have taken DSR on demand routing protocol to protect the network from any kind of malicious activity. In this first we authenticate the nodes by implementing digital signature, due to which only authenticated nodes can communicate in the network. Secondly we ensure the quality of communication by monitoring the action of nodes. Here we consider overhead percentage and packet delivery ratio as matrices. We simulate the environment in NS2 and results are extracted using awk scripts.

KEYWORDS-LAN, MANET, DSR

1. INTRODUCTION:

ADHOC means" for this purpose only". They can be setup anywhere without the need of any external infrastructure like base stations. There is increasing need of connectivity where there are no base stations or infrastructure where there ADHOC NETWORKS step in .An AD-HOC network is an autonomous collection of mobile nodes and wireless communication network is used to connect these mobile nodes. This type of network is known as MOBILE AD-HOC NETWORK (MANET). Nodes in MANET are mobile and communicate with each other via radio waves. Various characteristics of MANET are : communication via wireless means can be set up anywhere nodes can act as both router and host frequent routing updates.

DIGITAL SIGNATURE: The effectiveness of the proposed technique depends on the assumption that every node has a pair of private and public key. Public key is distributed over the network to every node exists. Whenever a packet is send to the network, it is signed by the sender so that authentication and integrity of that message is maintained throughout its lifetime.

NODE MONITORING: Every node maintains an action table associated with other nodes, which has an actual action, desired action and conclusion. Based on the conclusion generated in the action table nodes are inserted or ignored in the routing path. The proposed work is carried out on DSR protocol and is implemented in NS2

Node id	Actual action	Desired action	Conclusion
A	-	-	-
B	-	-	-
C	-	-	-

2.PROBLEM DEFINITION

A Mobile Adhoc Networks (MANET) is an autonomous collection of mobile nodes and there is no fixed infrastructure, so it is more vulnerable to attack and the problems related to the routing and security. Security is a primary concern in almost all the application scenarios and in order to provide the secure communication

between the mobile nodes. The open and dynamic nature of MANET makes it more vulnerable to attacks and cripples many MANET operations. Security plays an important role in mobile Adhoc networks because of its inherent vulnerabilities.

The research problem is how to provide security protection to the network. The major challenges include dynamic topology, decentralized control, limited resources, and the lack of information dissemination control.

The attacker doesn't allow the packet to arrive at real destination. In addition, the attacker produces some packets and sends them in the network to consume the bandwidth and create the bottleneck in th e network.

3.PROTOCOL USED IN SIMULATION:

DSR: The Dynamic Source Routing (DSR) protocol is an on-demand routing protocol based on source routing. In DSR, every mobile node in the network needs to maintain a route cache where it caches source routes that it has learned. When a host wants to send a packet to some other host, it first checks its route cache for a source route to the destination. In the case a route is found, the sender uses this route to propagate the packet.DSR basically works in two phases:

- ROUTE DISCOVERY
- ROUTE MAINTAINENCE

The request packet includes a request ID, the destination IP address, the route information about the source IP address, timestamp of the packet. The request is signed with the S's private key. If the route discovery is successful the initiating node receives a route reply packet listing a sequence of network nodes through which the request packet may reach the target.

In addition to the address of the original initiator of the request and the target of the request, each route request packet contains a route record, which accumulates a record of the sequence of hops taken by the route request packet as the request packet is propagated through the Ad hoc network during this route discovery. Each route request packet also contains a unique request ID, set by the initiator from a locally-maintained sequence number. In order to detect duplicate route requests received, each node in the Ad hoc network maintains a list of the initiator address, request ID pairs that it has recently received in any route request

4. SIMULATION APPROACH USED FOR RESULT ANALYSIS:

NETWORK SIMULATOR:

NS-2 is a discrete event network simulator in which physical activities are translated to events; events are processed in the order of their occurrences. The simulation time is progressed with the events getting processed. Typically, it can configure transport layer protocols, interface queues, routing protocols and also link layer mechanisms. We can easily see that NS2 provide us a whole view of the network construction and also maintains the flexibility for the user to decide or check. Thus, just this one software can help us simulate nearly all parts of the network. This definitely will save us great amount of cost invested on net work constructing.

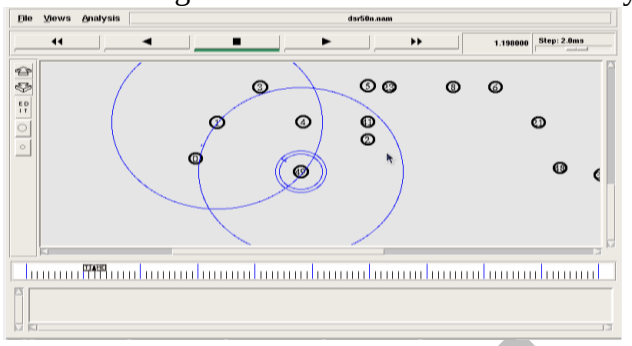
5. SIMULATION ENVIORNMENT

Parameters for Simulation Environment

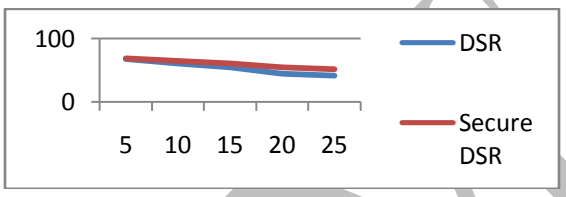
PARAMETER	VALUE
Traffic Type	TCP
Number of Nodes	50
Area Covered	1200 X 1200
Speed of the Node's	5,10,15,20,25 m/s
Routing Approaches	DSR
Mobility Type	Critical Mobility

ANIMATION:

We have created a network of 50 communicating mobile nodes based on te mobility speed.



GRAPHS:

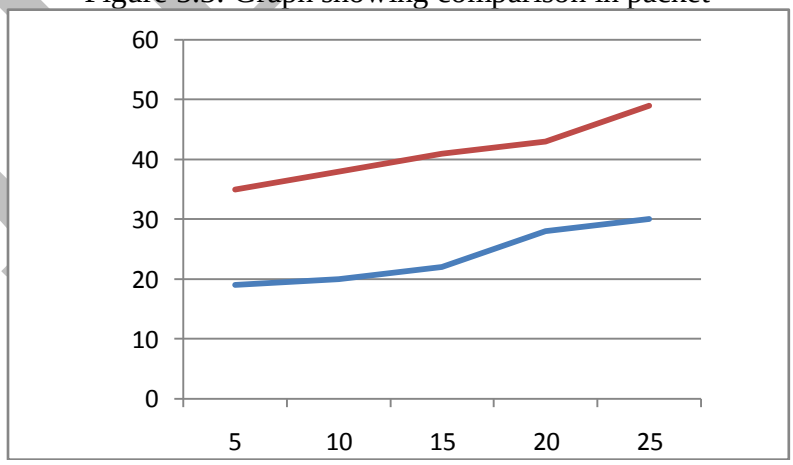


MOBILITY	DSR	Secure DSR
5	19	35
10	20	38
15	22	41
20	28	43
25	30	49

Figure 5.2: Graph showing %age overhead Vs Node Speed for 50 nodes

The above compared overhead percentages are of the scenarios when we analyses Secure DSR protocol with DSR protocol with no security

Figure 5.3: Graph showing comparison in packet



delivery ratio Vs Node Speed.

MOBILITY	5	10	15	20	25
DSR	68	61	55	45	42
Secure DSR	69	65	61	55	52

The above graph shows the packet delivery ratio with respect to speed of nodes. It is clearly shows that PDR (packet delivery ratio) is better in case of Secure DSR as compare to DSR.

6. CONCLUSION:

we propose an approach to protect the network communication from any kind of malicious activity. The effectiveness of the proposed technique depends on the assumption that every node has a pair of private and public key. Public key is distributed over the network to every node exists. Whenever a packet is send to the network, it is signed by the sender so that authentication and integrity of that message is maintained throughout its lifetime. Every node maintains an action table associated with other nodes, which has an actual action, desired action and conclusion. Based on the conclusion generated in the action table nodes are inserted or ignored in the routing path. The proposed work is carried out on DSR protocol and is implemented in NS2. Performance of proposed work in shown by calculating overhead percentage and packet delivery ratio by varying speed of the nodes.

REFERENCES:

1. Pallavi Sharma, Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Adhoc Network Using Digital Signature", IEEE 2011.
2. Pradnya Patange, S. P.Medhane, "PUBLIC KEY BASED APPROACH TO MITIGATE WORMHOLE ATTACK", International Journal of Computer Science Engineering Research and Development (IJCSERD).
3. Pravin Khandare, Prof. N. P. Kulkarni, "Public Key Encryption and 2Ack Based Approach to Defend Wormhole Attack", International Journal of Computer Trends and Technology- volume4Issue3- 2013.
4. Rutvij H.Jhaveri, Ashish D.Patel, Jatin D. Parmar, Bhavin I. Shah, " MANET Routing Protocols and Wormhole attack against AODV", IJCSNS International Journal of Computer Sciences and Network Security,VOL.(4),April 2010.
5. Yun Wang, Zhongke Zhang, Jie Wu, "A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information", Fifth IEEE International Conference on Networking, Architecture and Storage, 2010.
6. Reshmi Maulik and Nabendu Chaki, " A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications.
7. Shawkat K. Guirguis, Youssef A. Othman, "Simulation analysis of secure routing in Mobile Ad hoc networks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 9, November 2012.
8. C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008.
9. A.Jayanand, Prof.Dr.T.Jebarajan, "Performance Investigation and Analysis of Secured MANET Routing Protocols", International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012,3512-3516.
10. Kavitha Ammayappan, Vinjamuri Narsimha Sastry, and Atul Negi, "A New Secure Route Discovery Protocol for MANETs to Prevent Hidden Channel Attacks", International Journal of Network Security, Vol.14, No.3, PP. 121-141, May 2012.
11. G.Lavanya, A. Ebenezer Jeyakumar," An Enhanced Secured Dynamic Source Routing Protocol for MANETS", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume X, Issue-4, September 2011.
12. Huang Chuanhe, Li Jiangwei, and Jia Xiaohua, "A Secure Routing Protocol SDSR for Mobile Ad Hoc Networks", X. Jia, J. Wu, and Y. He (Eds.): MSN 2005, LNCS 3794, pp. 269–277, 2005.© Springer-Verlag Berlin Heidelberg 2005.
13. Thiyam Romila Devi, Rameswari Biswal, Vikram Kumar, Abhishek Jena, "IMPLEMENTATION OF DYNAMIC SOURCE ROUTING (DSR) IN MOBILE AD HOC NETWORK (MANET)", International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.
14. Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", IEEE 2003.
15. Mukesh Kumar, Naresh Kumar, "DETECTION AND PREVENTION OF DDOS ATTACK IN MANET'S USING DISABLE IP BROADCAST TECHNIQUE", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 7, July 2013