ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 1, Issue 2

Efficient Prevention Algorithm in MANET

Atul Kumar Agrawal, Ravindra Gupta, Gajendra Singh

Abstract - **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. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Dynamic Source Routing (DSR) algorithm is simple and best suited for high mobility nodes in wireless ad hoc networks. Due to high mobility in ad-hoc network, route may not exit for long time. Hence, DSR algorithm finds an alternative route when the existing communicating route goes down. It becomes a time consuming process if the communicating route fails frequently. This paper presents a new method to improve performance of DSR in Ad Hoc Network.**

Keyword: MANET, Flooding Attack, DSR

I. INTRODUCTION

The messy wired world now becomes smooth and clean atmosphere, due to use of wireless technology. The deployment cost, flexibility and less infrastructure makes the wireless technology, as the first choice for business, healthcare, education, war and many more fields of daily life. Wireless communication grouped into two main categories i.e. network with fixed infrastructure and network without fixed infrastructure [2]. A MANET represents a infrastructure-less distributed system that comprises wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ad-hoc network topologies, allowing people and devices to seamlessly internetwork with no pre-existing communication infrastructure and central administration. The success of mobile ad hoc networks (MANET) strongly depends on people's confidence in its security. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Dynamic Source Routing (DSR) algorithm is simple and best suited for high mobility nodes in wireless ad hoc networks. Due to high mobility in ad-hoc network, route may not exit for long time. Hence, DSR algorithm finds an alternative route when the existing communicating route goes down. It becomes a time consuming process if the communicating route fails frequently.

II. DSR

DSR is a reactive routing protocol which is able to manage a MANET without using periodic table-update messages like table-driven routing protocols do. DSR was specifically designed for use in multi-hop wireless ad hoc networks. Ad-hoc protocol allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration. Dynamic source routing (DSR) protocol is an on-demand routing protocol that is based on the concept of source routing [3]. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. The protocol consists of two major phases: route discovery and route maintenance.The function of DSR routing protocol is in this way: When two nodes which are not in wireless rang of each other, want to communicated with each other, if the source node has the related route to destination in its cache memory, it will insert The route in data packet headers and the packets will be sent from that specified route, and if it does have the related route to destination, it should begin the route discovery process. In route discovery process, route request packet (RREQ) is distributed in network until these packets reach the destination from one route. In this manner, as soon as receiving the first route request packet, destination sends the route reply packet (RREP) to the originator of RREQ. if a link is broken because of the motion of middle nodes, a route error packet is sent to the destination and destination tests another route, this task is repeated until the reply reaches the goal. Therefore, only after making error in current route, destination seeks another route. This mechanism causes delay in packet delivery.

III. FLOODING ATTACK IN MANET

As proactive routing protocols have already all the routes for destination nodes, that's why it has no issue for RREQ Flooding type of attacks, but reactive protocols (like AODV, DSR) arrange the route when node want to communicate with other node. RREQ scheme present in reactive protocols, initiate Flooding attacks that may be RREQ Flooding or Data Flooding attacks. In RREQ flooding attack, the attackers generate many RREQ packets in unit time to unknown IP address. As the priority of RREQ packets is higher than data packets, so the RREQ disposes first, this scenario becomes honey pot for an attacker. In data flooding, the attacker first maintains the routes to destination node, then sends frequently the useless data packets, which engage the network and stop the processing of legitimate data packets.

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 1, Issue 2

The MANETs are particularly vulnerable to DOS attacks, launched through compromised nodes or any attacker. The DOS attack against on demand routing protocols for MANETs are called Ad-hoc Flooding Attack [1]. The ad-hoc flooding attack is a new type of attack, introduced in 2005 by Ping Yi in his paper "Resisting Flooding Attacks in Ad-hoc Networks" [1]. Basically the ad-hoc flooding attack is a DOS attack against all on-demand ad-hoc network routing protocols such as AODV or DSR. In this attack, an attacker either sends a penalty of route request packets (RREQ Flooding Attack) for a node ID generally who is not in the network to consume the bandwidth of the network. In ad-hoc network the path discovery process is based on the flooding of route request. In this attack the intruder first find those IP that's not exist in the network, then flooded massive numbers of RREQ for those void IP address without obeying the RREQ-RATELIMIT in per second. Also attacker no waited for RREP just flooding the RREQ to void IP. Therefore in ad-hoc flooding attack the whole network completely full with RREQ packets, threw by attacker.

IV. Proposed Work

The breakthrough in the use of wireless cellular systems use the Mobile AD-Hoc networks were proposed to provide robust and reliable routing services. The idea was considered to be perfect until the misbehavior of selfish node was discovered. In our work we have used the Dynamic Source Routing (DSR) routing protocol along with the trust estimation function.Various parameters which are used for trust estimation are: Total number of RREQ packet sent by the neighbor per unit time, total number of packet successfully transmitted by the neighbor, Ratio of number of packet received correctly from the neighbor to the total number of received packet.

V. Analysis and Result

In our work we used modified DSR as a routing protocol. In our simulation we used 50 nodes to form an ad hoc node and used the random waypoint mobility model for them. All the 50 nodes move in the 1500 x 300 region. We used 0/50/150 Pause Time and 20/50 mobility speed. The same network model is used to evaluate the effect of flooding attack and then our prevention algorithm. We had selected many scenarios to analyze the results so that we can better understand the behavior in presence of malicious node.

Table 5.1 Packet Ratio with Scenario

S. No.	Scenario	DSR (OLD)	DSR (NEW)
1	0 20	4.69	1.38
2	50 20	4.4	1.3
3	50 50	5.05	1.3
4	150 20	4.75	1.59
5	150 50	5.3	1.76

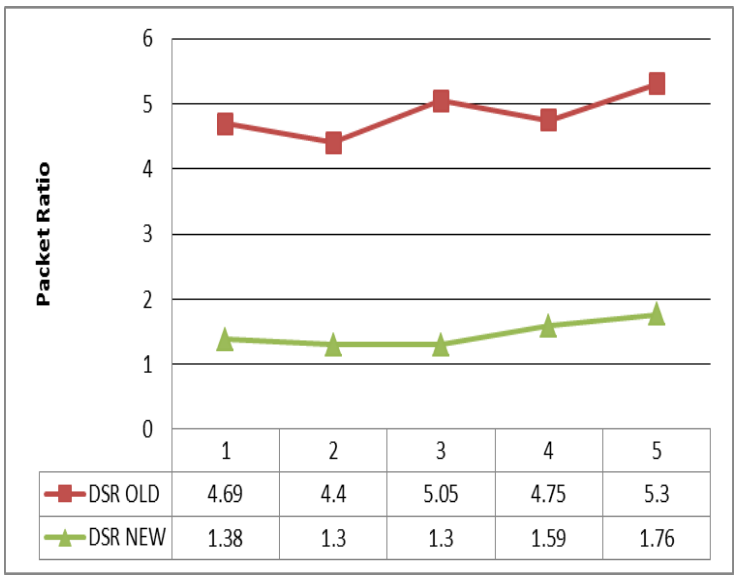

Fig 1: Packet Ratio with Scenario

VI. Conclusion

We compare the performance of original DSR protocol in presence of malicious node and the performance of proposed technique in presence of malicious node. In this Paper we used five different Scenarios. In these Scenario different mobility speed and pause time used. In this fig 5.1 accurate packet ratio is 1. Modified DSR has improved performance of MANET. The simulation results show that the new protocol has better performance than DSR protocol.

References

[1] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang,"Resisting Flooding Attacks in Ad Hoc Networks"Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) 0-7695-2315-3/05, IEEE, 2005

[2]Georgy Sklyarenko [MatrNr.: 3935701], "AODV Routing Protocol" Institut f¨ur Informatik,Freie Universit¨at Berlin,Takustr. 9, D-14195 Berlin, Germany

[3]D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[4]Sapna S. Kaushik 1 & P. R. Deshmukh 2, " Comparison of effectiveness of AODV, DSDV and DSR routing protocols in mobile Ad-Hoc Network" ",International Journal of Information Technology and Knowledge Management , Volume 2, No. 2 ,July-December 2009.

[5]P. Udayakumar and Asha Ambhaikar , " Experimenatal comparision of AODV and DSR protocols", International J. Of Engg. Research & Indu. Appls. (IJERIA) ISSN 0974 – 1518 vol. 2 No. III, 2009

ISSN 2249-6343
International Journal of Computer Technology and Electronics Engineering (IJCTEE)
Volume 1, Issue 2

[6]Nor Surayati Mohamad Usop, Azizol Abdullah and Ahmad Faisal Amri Abidin, " Performance Evaluation of AODV, DSDV & DSR Routing Protocol in grid Enviroment", IJCSNS International J. Of Computer Science and Network Security, Vol .9 No. 7 , July 2009.

[7]David Oliver Jorg "Performance Comparision of MANAT Routing Protocols In different Network Sizes", University of Beme , Switzerland, 2003