National Conference on Recent Research in Engineering and Technology (NCRRET-2015)
International Journal of Advance Engineering and Research Development (IJAERD)
e-ISSN: 2348 - 4470 , print-ISSN:2348-6406

Study of malicious node effect on Mobile Ad-hoc Network

Bhupendra B. Patel
Asst. Professor, Computer Science & Engineering Dept.
Dr. Jivraj Mehta Institute of Technology, Mogar,Anand

Abstract: ***The MANET stands for Mobile ad-hoc networks, as per user requirements it will connect or disconnect from network. The MANET is creating dynamic topology without any kind of centralized administration. The suitable routing protocol is crucial for improved communication in MANET. In MANET basically two types of routing protocols works for data transfer, the first one is reactive routing protocol and another one is proactive routing protocol. The MANET is work on open environment due to this reduce the routing protocol performance because the performance is effected by the malicious node. Malicious node either directly or indirectly affect to the network or routing performance. In various kind of attack happen on MANET environment like, Black hole attack, Denial of Service attack, eavesdropping, Sybil attack etc.***

Keyword: MANET, Malicious Node, Routing Protocol, attacks.

1. INTRODUCTION

An ad hoc network is typically distinct as an Infrastructure less network. It means that a network is absent the standard routing Infrastructure like fixed routers and routing backbones [1]. Generally, the ad hoc nodes are mobile and the essential communication standard is wireless. Every ad hoc node possibly will be able to of act as a router. Such ad hoc networks may happen in personal area networking, meeting rooms and battlefield operations, conferences etc..

Designing a well-organized and dependable routing protocol strategy is a huge challenge. Currently, [1] various ad hoc routing protocols have been proposed and developed by various researchers like DSDV, OLSR, TBRPF, AODV, DSR and ZRP. From all these, Ad-hoc On-demand Distance Vector (AODV) is recognized as one of the main IETF standards for MANET routing. AODV aims on improving routing performance, but provides only slight consideration to routing security, which indicates that it is susceptible to various attacks from malicious, compromised and selfish nodes. Currently, several efficient routing protocols have been projected. These protocols can be category into two categories: reactive routing protocols and proactive routing protocols. The reactive routing protocols, Ad hoc On Demand Distance Vector (AODV) protocol, nodes will find paths or routes only when required the data transmission. Another one is proactive routing protocols, Destination-Sequenced Distance-Vector (DSDV) Routing protocol, nodes find routes by periodic exchange of topology information.

In this paper, we survey the how to malicious node effect on MANET, that is, routing attacks such as DOS attack, Black hole attack, wormhole attacks etc.

2. ROUTING PROTOCOLS

The goal of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node. Routing protocols in a MANET can be classified into two categories: reactive routing protocols (e.g., AODV) and proactive routing protocols (e.g., DSDV) [3].In reactive routing protocols, nodes find routes only when they want to send data source to destination node whose route is unknown. On the other hand, in proactive protocols, nodes sometimes exchange topology information, and hence nodes can obtain route information any time they must send data. In this section, I describe standard routing protocols that currently being used.

AODV (Ad-hoc on demand distance vector):

[4]One of the most precious routing protocol for routing is the Ad-hoc on demand distance vector(AODV). AODV means it is a collection of Ad-hoc, ON demand, Distance and Vector. Ad-hoc means node movement or connection or disconnection with the networks at any time, On demand means when source wants to send data to the destination, Destination means find the distance between source to destination in term of number of hope counts, vector means list which store the node information. AODV

work on the OSPF method/algorithm. OSPF(open shortest path first) is based on the DISKJETRA's algorithm[5,6]. In AODV, at every node routing information are store.

AD-hoc Network routing protocols handle discovering, establishing, recovering and maintaining routing paths, In[6], AODV use some approaches for path or route establishment. Route Request(RREQ) Source node broadcast the route request message to neighbor node, neighbor node pass the message to specific destination. Route Reply(RREP) Destination Node unicast a route reply message to source. Neighbor node maintain the next entry for destination and forward the reply. In the case of multiple replies source node choose the shortest path with minimum hope count.

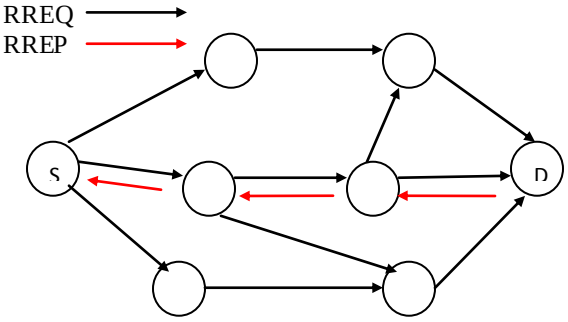

Fig. 2.1 AODV Routing Protocol With RREQ And RREP message.

Source sequence number and destination sequence number play a important role in AODV. Source node broadcast the packet with SSN and destination use DSN number which define the freshness of the path.

In the route maintenance when link are break, it broad casts a route error packet to its neighbor, when node receive route error message then source restart a route discovery process. In Fig.4.2 link break between A and D, So Node A inform or RERR to previous node that this link is broken chose another Shortest path.

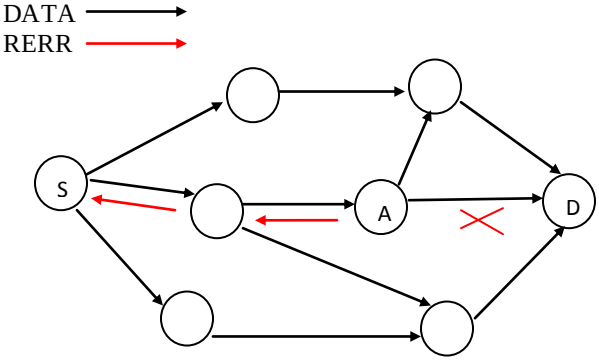

Fig.2.2 AODV Routing Protocol With RERR message

3. MALICIOUS NODE:

In[2] MANET, unhelpful node is malicious node. The nodes belonging to the first category are either faulty and doing misbehavior during operation, or are intentionally malicious and try to attack the system. Malicious node causes packet dropping, spread the false routing information. Various Effects of malicious nodes are given below:

- Malicious node reduces the network connectivity in MANETs.
- Reduce the network Performance
- No intention for energy-saving.
- Launch all kinds of denial-of-service (DoS) attacks by replaying, reordering or/and dropping packets from time to time, and even by sending fake routing messages.

4. ATTACKS ON MANET

Black Hole Attack:

In [8] a black hole attacks a malicious node advertising itself as having a valid route to the destination. With this intension the attacker consumes or intercepts the packet without any forwarding. An attacker can completely modify the packet and generate fake information, this cause the network traffic diverted or dropped[10].

Denial of Service Attack:

Denial of service attacks aim at the complete disruption of the routing function and therefore the whole operation of the ad-hoc network. The main instances of denial of service attack are making a service unavailable to user [4]. In a DOS attack the malicious node floods the network with fake route request packets in order to consume the resources of the participating node and disrupt the establishment of genuine routes. The sleep deprivation torture aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions [7].

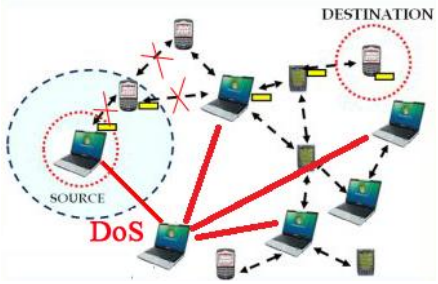

Fig. 4.1 DOS Attack

Eavesdropping attack:

This Eavesdropping is a passive attack. The node basically observes the Private data. This information can be later on used by the malicious or selfish node. The private information like public key, private key, password, location, can be fetched by the eavesdropping attack [9].

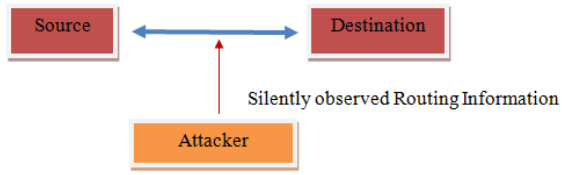

Fig. 4.2 Eavesdropping attack

Wormhole attack:

The attacker connects two remote parts of the ad hoc network using an additional communication medium as a tunnel. As a result two remote nodes believe they are neighbors and send data using the tunnel. The attacker has the option of conducting a traffic analysis or careful forwarding attack [10].

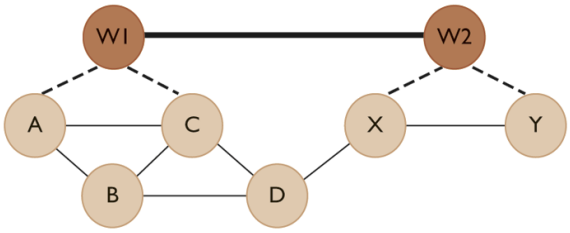

Fig.4.3 Wormhole attack

Distributed DOS attack:

A denial of service attack (DDOS) is recognized by its performance on a computer system or on a network that prevents actual use of its resources. A DDOS attack deploys many computers to initiate attack to complete its aim. Here many paths to execute a denial of service attack mainly common way is to send a flow of packets to the victim user and make the victim's user service busy. Another one path is to send a few twisted packets to the victim user machine so that its function get confused. DDoS attack can be performed at network level, operating system level, application level and many other level[11].

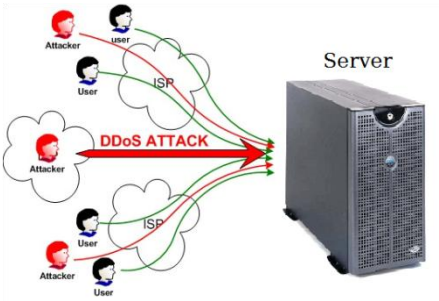

Fig.4.4 Distributed DOS Attack

5. CONCLUSION

Mobile Ad Hoc Network is a multi-hop wireless network, structuring a temporary network topology without any help from some recognized infrastructure or centralized administration. Because of the lack of several dedicated routers, each node needs to donate towards the configuration and protection of the routing framework. In MANET, no centrally administered secure routers, attackers can attack the network with ease. To overcome this better routing protocol must be used. AODV is the widely used routing protocol for MANET. Due to some misbehavior of malicious node the routing performance would be decreases.

6. REFERENCES

[1] Datuk Prof Ir Ishak Ismail ,Mohd Hairil Fitri Ja'afar,"Mobile Ad Hoc Network Overview"2007 ASIA-PACIFIC CONFERENCE ON APPLIED ELECTROMAGNETICS PROCEEDINGS December 4-6, 2007, Melaka, MALAYSIA 1-4244-1435-0/07/$25.00©2007 IEEE

[2] S.Gopinath, Dr.S.Nirmala & N.Sureshkumar "Misbehavior Detection : A New Approach for MANET"International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622,Vol. 2, Issue 1,Jan-Feb 2012, pp.993-997

[3] Saleh Ali K.Al-Omari, Putra Sumari " An Overview Of Mobile Ad Hoc Networks for the existing protocols and application",Journal on Applications of Graph Theory in Wireless Adhoc Networks and Sensor Networks(JGRAPH-HOC) Vol.2, No.1, March 2010

[4] Bhupendra Patel, Anurag Gupta, Nabila Hyder, and Kamlesh Rana, "AODV Routing Protocol Performance in Malicious Environment",M.K. Kundu et al. (eds.),

Advanced Computing, Networking and Informatics - Volume 2, Smart Innovation, Systems and Technologies 28, DOI: 10.1007/978-3-319-07350-7_23, © Springer International Publishing Switzerland 2014

[5] Al-Omari, S.A.K., Sumari, P.: An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Application. Journal on Applications of Graph Theory in Wireless Ad-hoc Networks and sensor Networks 2(1) (2010)

[6] Sheikhl, R., Chandee, M.S., Mishra, D.K.: Security Issues in MANET: A Review. In: 7th International Conference on Wireless and Optical Communications Networks (2010)

[7] Kumar, V., Sharma, R., Kush, A.: Effect of Malicious Nodes on AODV in Mobile Ad Hoc Networks. International Journal of Computer Science and Management Research 1(3) (2012)

[8] Bhupendra B Patel, Department of Master of Engineering, (Wireless and Mobile Computing), GTU, Ahmadabad, Gujarat. "Study of Malicious Node in AODV Routing Protocols" International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 2, No. 5, May 2013

[9] Rashid Sheikhl Mahakal Singh Chandee, Durgesh Kumar Mishra,"Security Issues in MANET: A Review"IEEE

[10] BOUNPADITH KANNHAVONG, HIDEHISA NAKAYAMA, YOSHIAKI NEMOTO, AND NEI KATO, "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS"SECURITY IN WIRELESS MOBILE AD HOC AND SENSOR NETWORKS,IEEE Wireless Communications • October 2007 1536-1284/07/$20.00 © 2007 IEEE

[11] Arun Raj Kumar, P. and S. Selvakumar "Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms" 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009 , 978-1-4244-2928-8/09/$25 .00 © 2009 IEEE.