International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Routing in MANET and the Various Threats: A Survey

Anita[1], Abhilasha[2]

Department of CSE, GZS PTU Campus, Bathinda, Punjab, India

Abstract: ***Wireless network is a network established using radio signal frequency to communicate among computers and other network devices. One such network is MANET which is a self configuring infrastructure-less network of mobile devices connected wirelessly. Wireless adhoc network like MANET consists of a number of mobile nodes that communicate with each other without the help of any fixed infrastructure or centralized network. Each device is free to join or leave the network whenever required. Therefore in this case, security is a big issue as the chances of attacks are severe. Various routing protocols used to set up a wireless connection are Reactive protocols like DSR, AODV, TORA and then the proactive protocols like DSDV, OLSR. Also there are the hybrid protocols that include ZRP. Any of these can be used for routing as per the requirement of the network. The various attacks are possible when it comes to a network like MANET. These may be Black hole attack, Grayhole attack, wormhole attack, Selective packet drop. Selective packet dropping attack is very complex and difficult to isolate. We discuss various algorithms and methods to identify selective packet drop in MANET and isolate it as much possible. We also compare methods for further improvement in the same.***

Keywords: MANET, Adhoc network, Selective packet drop, AODV

1. Introduction

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure or any centralized administration. There is no stationary infrastructure or base station for communication. Each node itself is responsible for routing of data packets to/from other nodes. The mobile nodes in the network dynamically establish the routing in an ad hoc network. There is the possibility of more security threats in case of mobile and ad hoc networks (MANET) as compare to centralized wireless networks. A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless connection. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. The primary challenge in building a MANET is to equip each device to continuously retain the information required to properly route traffic. The mobile nodes that are in radio range of each other can directly communicate, whereas can communicate through intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and robust.

2. Various Routing Protocols

An One of the most important and a difficult mechanism in ad hoc networking is the routing mechanism. The nodes in the network have to set up a route for themselves as there is no prior information of the network topology. Routing protocols in MANETs are classified into three different categories according to their functionality.

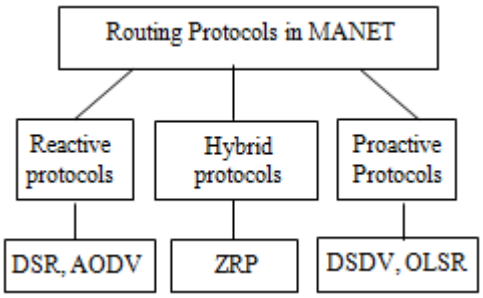

Figure 1: Classification of Routing Protocols in MANET

a. Reactive protocols

These are also called as on demand routing protocols. These do not establish a connection unless there is communication required in the network. The connection is established and destroyed as required by the mobile nodes. It means that it creates the routes only when desired by the source node. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The various protocols that are reactive are DSR(Dynamic Source Routing), AODV(Ad hoc On Demand Protocol), TORA(Temporally-Ordered Routing Algorithm). AODV is an on-demand routing protocol used in ad hoc networks. This protocol is like any other on-demand routing protocol which facilitates a smooth adaptation to changes in the link conditions. In case when a link fails, messages are sent only to the affected nodes. With this information, it enables the affected nodes invalidate all the routes through the failed link.

b. Proactive protocols

In these protocols the routes are established even before any communication is carried out in the network. They attempt to maintain up to date information from each node to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. Proactive routing protocols are table driven routing protocols. These protocols require nodes

to send control packets periodically to maintain the routes. To maintain all possible routes in a network is difficult because the control packets for route maintenance consume a lot of bandwidth on links where there is no need of data transfers. The most familiar types of the proactive type are destination sequenced distance vector (DSDV) routing protocol and optimized link state routing (OLSR) protocol.

C. Hybrid Protocols

This type of protocols combines the advantages of proactive and of reactive routing. These include protocols like Zone Routing Protocol (ZRP).

3. Attacks in MANET

As the MANET is prone to threats, various attacks possible are discussed here. The attacks can be classified as active or passive attacks, internal or external attacks, or different attacks classified on the basis of different protocols. A passive attack does not disrupt the normal operation of the network. The attacker only snoops the data exchanged in the network without altering it. It includes Eavesdropping, jamming and traffic analysis and monitoring. In case of active attacks, the attacker attempts to alter or destroy the data being exchanged in the network. This attack disrupts the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks .The ultimate goals of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, authentication, non-repudiation, and availability to mobile users.

Active Attacks	Black hole attack, modifications, wormhole etc
Passive Attacks	Eavesdropping, jamming, traffic analysis and monitoring

Figure 2: Classification of attacks in MANET

4. Selective Drop Attack

Selective packet dropping attack is a severe attack that lets the selfish node to send a few packets to the next node while dropping the rest of the packets. Such an attack is very difficult to identify and isolate completely. . Selfish node also drop packet in their different ways. They drop packets only to save their resources not damage any other nodes. Selective forwarding attacks may damage some mission of applications. In these types of attacks, malicious nodes act as normal nodes every time but selectively drop sensitive packets, such as packet coverage the movement of the differing forces. Such selective dropping is tough to detect. Selective forwarding attack is complex attack to detect, since packet drops in sensor networks may be caused by untrustworthy wireless communications or node failures.

5. Literature Review

Various methods have been used to detect and isolate the attacks in MANET. There are various advantages and disadvantages which will help us for further improvement in this field. The sequence numbers of the destination nodes are calculated. Attackers change the sequence number and that's how the attacks are detected and then can be isolated using various factors of the sequence numbers. This can also be simply dealt with by changing the path of the source to destination for further communication. Various papers discuss the vulnerabilities, challenges and attacks in MANET networks. There are number of attacks and different ways of dealing with the attacks. In another paper they discussed about the defensive mechanisms based on cumulative acknowledgement and energy based is proposed to detect selective forward attack in mobile wireless sensor networks. The scheme is evaluated in terms of packet delivery ratio and throughput. The malicious node is detected based on the acknowledgement and energy level of the node. The energy consumption of the detection scheme is less when compared with existing detection schemes. In yet another paper, the technique of sending the control packets before data is being involved in a way that the data can be sent only when the source and destination nodes are synchronized.

6. Future Scope

A number of algorithms that have been discussed in case of Selective packet drop attack have both advantages and disadvantages. The future scope lies in finding a technique that will avoid the problem before it arises. So we tend to find out a technique that avoids the attack that happens to selectively forward some packets while keeping the others. So it is best to derive an algorithm that will prevent and isolate this attack as much as possible.

7. Conclusion

As we have seen that mobile ad hoc networks are the self configuring networks in which the nodes can independently join and leave the network. There is no fixed infrastructure and therefore no centralized controller is required in such networks. They are versatile, dynamic and robust networks. Various protocols like AODV, DSR, TORA, ZRP, DSDV, OLSR are used based on the type of network and its requirements. Also because of no fixed infrastructure, it is possible to attack MANET easily. Attackers find it easy to destroy data in these networks as they are difficult to identify and isolate. We have seen various active and passive attacks which pose these problems. These attacks may include blackhole attack, grayhole attack, wormhole attack, selective packet drop attack. The selective packet drop attack is a major issue that is being dealt using different methods and algorithms. Many research works have been done to identify as well as isolate this. Here we have compared techniques used by different people and the various improvements in this field. We also propose to do some research in identifying the attack using the diffie Hellman algorithm and try to isolate it if possible in the further work. Our main aim is to establish a network that will have secure connections from source to destination so that data can be transferred without

any delay and we can also increase the throughput of the network.

References

[1] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.
[2] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, volume 5, Number 3, 2007, pp 338-346.
[3] Priyanka Goyal, Vintra Parmar and Rahul Rishi , " MANET: Vulnerabilities, Challenges, Attacks, Application" , *IJCEM International Journal of Computational Engineering & Management*, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011
[4] S. Sharmila and G. Umamaheswari, " Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", *International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012*
[5] LathaTamilselvan and V Sankarnarayana, " Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp 13-20.
[6] S.Marti, T.J.Giuli, K.lai and M.bakery "Mitigating routing misbehaviour in mobile ad hoc networks", 6th MobiCom, Boston, Massachusetts, August 2000.
[7] Caimu Tang ,Dapeng Oilver "An Efficient Mobile Authentication Scheme for Wireless Networks",*IEEE*, 2011
[8] N.Bhalaji and Dr.A.Shanmugam, "Reliable Routing against Selective Packet Drop
[9] Attack in DSR based MANET", JOURNAL OF SOFTWARE, VOL. 4, NO. 6, AUGUST 2009
[10] Rusha Nandy, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" *International Journal of Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043, 2011*
[11] Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks" , *10th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648, n.d.*
[12] Sevil Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", *IEEE, 2010*

Author Profile

Anita is M-Tech Scholar of GZS PTU Campus, Bathinda. She has completed B-Tech from GZS PTU Campus, Bathinda in 2010.

Er. Abhilasha Associate Professor (CSE) GZS PTU Campus, Bathinda. She is also head of department (CSE) GZS PTU Campus, Bathinda. She has completed her M-Tech and B-Tech and joined the Campus in 1998.she is serving as the head of Department since Jan 2013.