IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-4 E-ISSN: 2347-2693

To Study the Various Attacks and Protocols in MANET

Harkiranpreet Kaur[1*] and Rasneet Kaur[2]

[1*2]Department of Computer Science & Engineering, PTU, India

Available online at: www.ijcseonline.org

Received: Mar/22/2016 Revised: Apr /02/2016 Accepted: Apr/14/2016 Published: Apr/30/2016

***Abstract*—** MANET is a network which has no central coordinator and the nodes are free to move in any direction because there is no fixed infrastructure. There are various types of attacks which can easily harm the security of the network. Sender sends a packet to the destination by using the best path with the help of routing protocols. In this review paper, numerous attacks will be discussed.

Keywords- MANET, Attacks, DSR, infrastructure-less

I. INTRODUCTION

Wireless Networks term is refers to a kind of networking that do not requires cables to connect with devices during communication. The transmission is take place with the help of radio waves at physical level. Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols and without the using of cables. It is also known as Wi-Fi or WLAN. With the help of this network, devices can be joined easily with the help of radio frequency without wires to sharing information [4]. They have ability to self-configure makes this technology suitable for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is urgently required. In MANET routing protocols for both static and dynamic topology are used.

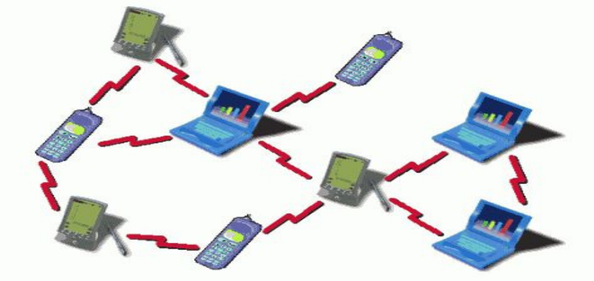

Fig 1.1 MANET

As MANETs are illustrated by limited bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes, topology changes and unreliable communication in the design. There are many types of protocol are available in MANET. Its efficiency of a routing protocol is determined by its battery power consumption of a participating node and routing of traffic into the network.

Mobile Ad hoc Network is a mobile multi-hop which is wireless distributed network and self- organized in nature. The primary objective of routing protocol is to discover the route. In the routing protocol for MANET undertakes to setup and maintain routes between nodes. In MANET, constantly changing network topology causes link breakage and invalidation of end-to-end route. There is highly dynamic nature of wireless network imposes severe restrictions on routing protocols.

1.2 TYPES OF MANET

1. Vehicular Ad Hoc Networks: These are used for the communication among the mobile vehicles. The communication being carries on even if the vehicles are moving in the different direction with in a particular area.
2. Intelligent Vehicular Ad hoc Networks (InVANETs) : It is used in case like collision of the vehicles or any other types of mobility problems. It is uses the scheme intelligently and the flow less communications goes on.
3. Internet Based Mobile Ad hoc Networks (iMANET): It is an ad hoc networks that connection mobile nodes and fixed nodes of Internet-gateway. Ad hoc routing algorithms don't apply directly in such type of networks.

1.3 ATTACKS ON MANET

There are two types of attacks are present in MANET which break the security of the networks. These attacks are as follow:
1. Passive Attacks: A passive attack obtains data exchanged in the network without disturbing the communications operation. The passive attacks are difficult to detection. In its, operations are not affected. The operations supposed to be accomplished by a malicious node ignored and attempting to recover valuable data during listens to the channel. Examples of Passive Attacks are snooping and eavesdropping.
2. Active Attacks: An active attack is that attack which any data or information is inserted into the network so that information and operation may harm. It involves

modification, fabrication and disruption and affects the operation of the network. Examples of active attacks are spoofing, impersonation etc.

3. Internal Attack: In an internal attack from the network the malicious node gains unauthorized access and behave as a genuine node. Internal attacks are as of compromised nodes that are part of the set of connections. Traffic can be analyze between other nodes and may participate in the activities of other networks.

4. External Attack: The external attack is conceded out by the nodes which do not belong to network. It may cause unavailability of the network and congestion by sending false information for the network.

5. Wormhole Attack: In wormhole attack, a malicious node, at one location in the network receives packets and to another location in the network tunnels them, to the location where packets are present into the network. When the control messages are routing are tunneled it create disrupted. It is a network layer attack. The two colluding attacker's tunnel between them is referred as wormhole.

6. Black hole Attack: In this type of attack the requests is listen by an attacker for the routers in a flooding based protocol .When a request is received by the attacker to the destination node for a route, it creates a reply for the short route and enters into the passageway to do something with the packets passing between them.

7. Denial of Service Attack: The aims of attack are to hit the accessibility of a node and all the nodes in the entire network. The services will not be accessible if the attack is successful. The attacker generally uses battery exhaustion method and radio signal jamming.

8. Byzantine Attack: In this attack, an intermediate compromised node carries out attacks such as creating collision forwarding packets on non-optimal paths, routing loops, and dropping packets selectively which result in interruption or dreadful conditions of the routing services.

9. Jamming Attack: In this attack, attacker wireless medium keep monitoring initially in sort to verify frequency at which destination node is getting signal from sender. Signal is transmit on that frequency to hindered error free receptor.

10. Man- in- the- middle attack: In this attack, an attacker sits between the sender and receiver and any information being sent between two nodes sniffs by him. In some cases, attacker may masquerade as the sender to communicate with receiver or masquerade as the receiver to reply to the sender. It starts when first attacker sniffs and eavesdrops the packets.

11. Replay Attack: In this type of attack an attacker performs a replay attack are repeatedly re-transmitted the valid data to the network injection fort routing traffic that has been previously captured. This attack targets the routes freshness and determines poor security design.

12. Gray-hole attack: This attack is also known as routing misbehavior attack. It leads to messages dropping. It has two phases. In the first phase a valid route to destination is advertise by nodes itself. In second phase, with a certain probability nodes drops intercepted packets.

II. LITERATURE REVIEW

I In this paper, they have proposed a new model based on the measuremeasure of correlation among the error and the correct reception times in order to detect the presence of jamming attack in ad hoc networks. The correlation is defined here, as a measure of the association between two random variables. Main purpose is to detect specific type of jamming, in which the jammer transmits only when valid radio activity is signaled from its radio hardware, which it represents the major case of such attack. The simulation results of the model are quite promising. In fact, we have been able to detect the presence of jamming with very high degree of confidence. Our objective in the future is to use our approach to detect others DoS attacks, and to find an effective reaction mechanism to cope up with jamming.

They have addressed the problem of control-channel jamming in multi-channel ad hoc networks, under node compromise. We proposed a randomized distributed channel establishment scheme that allows nodes to select a new control channel using frequency hopping. Our method differs from classical frequency hopping in that the communicating nodes are not synchronized to the same hopping sequence. Instead, each node follows a unique hopping sequence. They showed that their scheme can uniquely identify compromised nodes through their unique sequence and exclude them from the network. We evaluated the performance of our scheme based on the newly proposed metrics of evasion entropy, evasion delay, and evasion ratio. The proposed scheme can by utilize as a temporary solution for the control channel re-establishment until the jammer and the compromised nodes are removed from the network.

In this paper, they have discussed various mutual authentication schemes of mobile ad hoc network. They had discussed the symmetric key and asymmetric key distribution schemes. They had also discussed PKI (public key distribution) scheme which based on the symmetric key distribution scheme.

They proposed, a protocol extension of 802.11 DCF protocol to detect the selfish behavior of the nodes in the infrastructure and ad hoc network topologies. Selfish nodes means the nodes which select the conventional window (CW) time in such a way so that the other nodes are keep on waiting to send the data and overall through put of the network degrade. The proposed scheme has three components first one is that the receiver decides that whether sender is diverting form protocol or not. Second component is penalize ,in this scheme the receiver assigns the conventional window time to the sender if sender not sends data in that time period sender have to pay the plenty.

They have discussed about the Mobile ad-hoc network is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. Due to brutal challenges, the special features of MANET bring this technology great opportunistic together. This paper describes the essential problems of ad hoc network by including the idea, features, category, and vulnerabilities of MANET. This paper presents an overview and the study of the routing protocols. Also include the several challenging issues, emerging application and the future trends of MANET.

III. DSR PROTOCOL

DSR is a reactive routing protocol for ad hoc wireless networks. It also has on-demand features like AODV but it's not table-driven. It is based on source routing. The Dynamic Source Routing protocol (DSR) is a simple designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes and efficient routing protocol.

DSR allows the network to be fully self-organizing and self-configuring. Dynamic Source Routing protocol allows finding a source route across multiple networks nodes to dynamically.

In this each data packet carries in its header completely, nodes list of nodes through which the packet must pass dynamically ordered, allowing loop-free packet routing and the need for up-to-date routing information in the intermediate nodes avoiding through which the packet is forwarded.

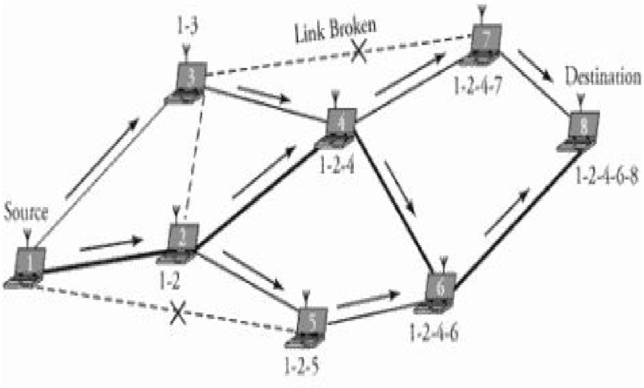

Fig 3.1 DSR Protocol

IV. CONCLUSION

Currently, the biggest challenge in Mobile Ad-hoc Network is its security which is in threat due to its limitations like absence of central coordinator, limited bandwidth, open media etc. There are various kind of security attacks are possible in the Ad-hoc network. These are very harmful for the security of the network. DSR protocol is used to choose the best path between the sender and the destination on the basis of hop count and sequence number. Various techniques are established to detect and isolate these attacks, but still MANET is not completely secure network.

REFERENCES

[1] Ali Hamieh, Jalel Ben-Othman, "*Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution*", IEEE, 2009

[2] Amandeep Singh Bhatia and Rupinder Kaur Cheema,"*Analyzing and Implementing the Mobility over MANETS using Random Way Point Model*",International Journal of Computer Applications (0975 – 8887) Volume 68– No.17, April 2013

[3] Singh, Umesh Kumar, et al. "An Overview and Study of Security Issues & Challenges in Mobile Ad-hoc Networks (MANET)." *International Journal of Computer Science and Information Security*, Volume-9, No- 4 (2011): 106-110.

[4] Neeraj Kumar Pandey and Amit Kumar Mishra, "An Augmentation in a Readymade Simulators Used for MANET Routing Protocols: Comparison and Analysis", *International Journal of Computer Sciences and Engineering,* Volume-02, Issue-03, Page No (60-63), Mar -2014, E-ISSN: 2347-2693

[5] Caimu Tang,Dapeng Oilver "*An Efficient Mobile Authentication Scheme for Wireless Networks*",IEEE, 2011

[6] Dr. A.K Verma, "*Mobile Adhoc Networks: An Introduction*", 2003

[7] Erik G. Nilsson and Ketil Stølen, "*Ad Hoc Networks and Mobile Devices in Emergency Response – a Perfect Match*"

[8] Sharma, Pradeep Kumar, Shivlal Mewada, and Pratiksha Nigam. "Investigation Based Performance of Black and Gray Hole Attack in Mobile Ad-Hoc Network." *International Journal of Scientific Research in Network Security and Communication*, Volune-1. Issue-4 (2013): 8-11.

[9] Ian D. Chakeres and Elizabeth M. Belding-Royer , "*AODV Routing Protocol Implementation Design*", In C. E. Perkins, editor, Ad hoc Networking, pages 173.219. Addison-Wesley, 2004

Authors Profile

Harkiranpreet Kaur has completed her Bachelor of Technology from I. K. Gujral Punjab Technical University, India in 2013 and is pursuing her Master of Technology from I K Gujral PTU.

Rasneet Kaur has completed her Master of Technology from Punjabi University, Patiala, India and is working as an assistant professor in Shaheed Udham Singh College of Engineering & Technology, Tangori (Mohali).