A Survey of Black hole Attack in Mobile Ad-hoc Network

Er. Dangat Ganesh D., Prof. Jayanti E

***Abstract*— Mobile Ad hoc Networks (MANET) has become an exciting and important technology in recent years because of the rapid proliferation of wireless devices. A mobile Ad hoc network consists of mobile nodes that can move freely in an open environment. Communicating nodes in a Mobile Ad hoc Network usually seek the help of other intermediate nodes to establish communication channels. In such an environment, malicious intermediate nodes can be a threat to the security of conversation between mobile nodes. The security experience from the Wired Network world is of little use in Wireless Mobile Ad hoc networks, due to some basic differences between the two Networks. Therefore, some novel solutions are required to make Mobile Ad hoc Network secure.**

Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET).In this paper, we are discuss the Black Hole attacks to the best of our knowledge.

***Index Terms*— Black hole attacks, MANET, Survey, Security.**

I. INTRODUCTION

Ad-hoc Networks; They have no any infrastructure ,where any node can be join into the network or it will be left from the network any time.it is really a free network having any kind of infrastructure or less infrastructure. In such type of network there is no central administrator to manage the network. They have capability to create the network & destroy it Ad hoc network Categories into following types [3].

1.Static Ad hoc Network.
2.Mobile Ad hoc Network.

1. Static Ad hoc Network:-

In the static ad hoc network workstation & the geographic Location are not moving from one place to another they are fixed. That's why they are known as static Ad hoc Network.

2. Mobile Ad hoc network:-

It is a collection of mobile device which will be continuously moving from one location to the other location. Whenever any mobile will enter into the network then it will form the network without any central administrator. Following are the some characteristic of MANET [5].

1. Self-Organizing
2. Self-Configuring Multi hop wireless network
3. No geographical restriction
4. One of the limitations of MANET is limited energy resource of the node.

Manuscript received September 18, 2014.
Er. Dangat Ganesh D. SCOE, Pune.
Prof. Jayanti E. Assit. Professor, SCOE, Pune.

Fig 1 shows the Architecture of MANET

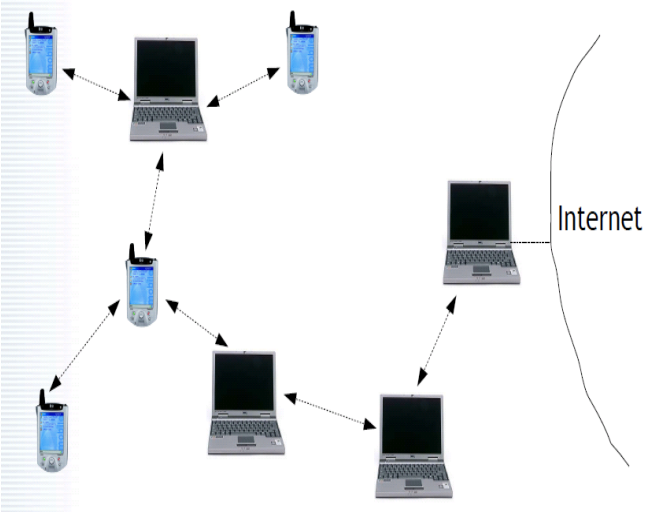

Fig.1 Mobile Ad hoc Network

II. SECURITY REQUIREMENT FOR MANET

There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment [7]. They are mainly: Same thing will be require for MANET as compare to the fixed station like:

1. Confidentiality
2. Availability
3. Authentication
4. Integrity
5. Non Repudiation

Confidentiality: Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediates nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

Availability: Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services.

Authentication: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

Integrity: Message being transmitted is never altered.

Non-repudiation: Ensures that sending and receiving parties can never deny ever sending or receiving the message.

III. LAYER WISE CLASSIFICATION OF ATTACK IN MANET

To many attack will be occur into the network out of these some attack can be classified according to the network protocol stack is as follows,

Sr. No	Layer	Attack occur in that Layer
1	Application Layer	Repudiation, data corruption
2	Transport Layer	Session hijacking, SYN flooding
3	Network Layer	Wormhole, black-hole, Byzantine, flooding, resource consumption, location disclosure attacks
4	Data link Layer	Traffic analysis, monitoring, disruption MAC (802.11),WEP weakness
5	Physical Layer	Jamming, interceptions, eavesdropping
6	Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

Table 1 Layer wise classification of attack in MANET

IV. BLACK HOLE ATTACK IN MANET

In the Black hole attack a malicious node which make the use of vulnerabilities of the route discovering packet of the routing protocol to which discover as a shortest path to the node. Also it intercepts the packet of any other node or whichever it wants. In this the malicious node gives reply to the source node. The source node gives the reply to the malicious node at that time source node will not check the routing table so the source node think that he discovery process is completed & ignore the other route reply message from other node & select the false route. So that the false node do this by assigning a high sequence number to the reply packet then the false node will drop the all received message instead of relaying as a protocol require[10].

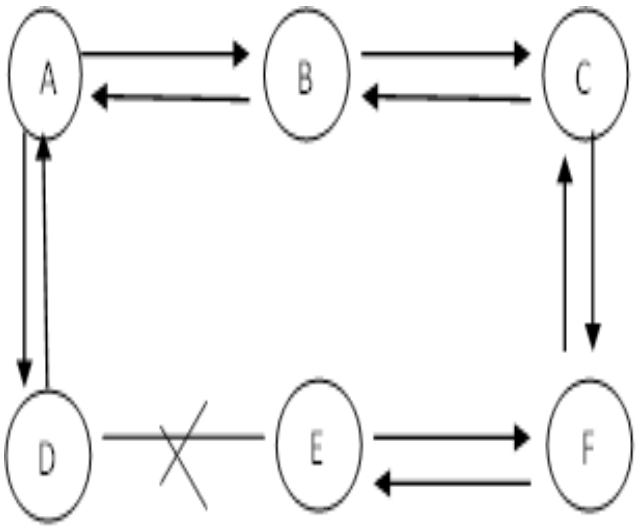

Fig. 2 Black Hole Attack in MANET

False node in the network take all the routing information & route request Message so that quality of routing information is available to the false node. This False node is called as black hole node. Figure 2 shows how black hole attack will arise in the network. Source node A send the RREQ message in to the network & initiate the route Discovery process. In that if C node is a false node then it will gives the RREP message to the source node before any other node will gives the reply to the source node as soon as the reply get from the node C, source will gives the reply to the Node "C" & think that C is having the active link to the Destination node & discovery is complete & now A will ignore the All the reply message will be come from the other node & A will start the communication with the C & it will confused or lost the all the data packet

V. CONCLUSION

MANET require a reliable, efficient & scalable & most importantly a secure protocol as they are highly insecure, Self organizing, rapidly deployed & they use dynamic routing mobile ad hoc network is likely to be attacked by the black hole attack There are so many technique to improve the data security in mobile ad hoc network.

REFERENCE

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE, vol. 11, no. 1,

[2] P. Goyal, S. Batra, and A. Singh.A literature review of security attack in mobile ad-hoc networks. International Journal of Computer Applications IJCA, 9(12):24–28.

[3] Khin Sandar Win,"Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 48, 2008. S.J. Sultanuddin, et al International Journal of Computer and Electronics Research [Volume 2, Issue 2, April 2013] © http://ijcer.org ISSN: 2278-5795 Page 93

[4] Yih-Chun Hu, A. Perrig, D.B.Johnson, "Wormhole attacks in wireless networks", Selected Areas in Communications, IEEE.

[5] N Sitapara& Prof. S B. VanjaleInternational Conference, ICETE-2010 on Emerging trends in engineering on 21st Feb 2010organized by J.J.Magdum College Of Engineering, Jasingpur "Detection and Prevention of Black Hole Attack in Mobile Ad- Hoc Networks".

[6] E. A. Mary Anita and V. Vasudevan, Black Hole attack on multicast routing protocols, JCIT, Vol.4, No.2, pp. 64–68.

[7] H.Nakayama, S.Kurosawa, A.Jamalipour, Y. Nemoto, and N. Kato.A dynamic anomaly detection scheme for aodv based mobile ad hoc networks. Vehicular Technology, IEEE Transactions on, 58(5):2471 –2481, jun 2009.

[8] P.N. Raj and P.B. Swadas. Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. Arxiv preprint arXiv:0909.2371, 2009.

[9] A. Baadache and A. Belmehdi. Avoiding black hole an cooperative black hole attacks in wireless ad hoc networks.

[10] Ramaswamy Sanjay,Fu Huirong, Sreekantaradhya Manohar, Dixon John and Nygard Kendall: Prevention of Cooperative BlackHole Attack in MANET. Department of Computer Science,IACC 258 North Dakota State University,Fargo,58105,March2003,pages 7.