IJCAT - International Journal of Computing and Technology, Volume 3, Issue 5, May 2016
ISSN : 2348 - 6090
www.IJCAT.org

A Review on Various Attacks in Manets

[1] Navpreet Kaur, [2] Puneet Kumar

[1] Student (M.Tech), Department of CSE
Sri Sai College of Engg. & Technology, Manawala,
Amritsar, Punjab, India

[2] Assistant Professor, Department of CSE
Sri Sai College of Engg. & Technology, Manawala,
Amritsar, Punjab, India

Abstract - A Mobile-Adhoc network is the temporary network in which set of nodes which can communicating with each other using wireless channels and it has no fixed infrastructure. For communication purpose devices or nodes can be used routing protocols like AODV, DSDV, DSR etc. but main issues of security against routing in manets that is Black hole attack , flooding attack, wormhole attack, greyhole attack. Attacks in which malicious node can provide the fake path during routing process and then packets drops later and also decrease the network performances. So in this paper, we survey the various attack in Manets which is considerable security issues.

***Keywords* - Manets, Black Hole, Flooding, Grey Hole, Wormhole.**

1. Introduction

Manets is an independent system, where a number of mobiles nodes are connected with each other through wireless links. Intermediate nodes also help for transmit the information between the nodes [3]. Nodes have no restriction to join or leave the network freely due to its Dynamic nature of its topology. Due to dynamic topology, node mobility, self-organizing capability, these are all characteristic's of Manets which differentiate it from other networks [9].

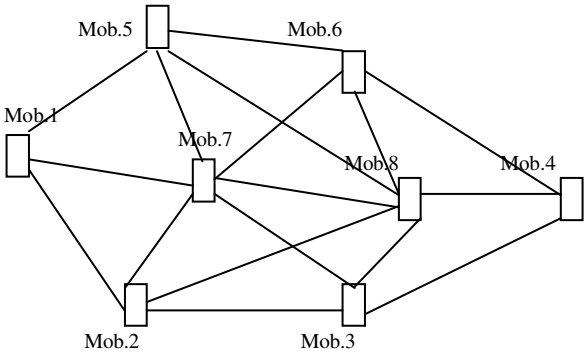

Fig.1 MANETs

2. Various Attacks

Manets suffer various types of attacks which decreases network performance like breakdown the node links, bandwidth; increase the latency of particular packet etc [9][11]. Firstly attacks are classified into two categories:
1. Active attacks
2. Passive attacks

Active Attacks : This is the type of attacks in which fake data or information are inserted in to the network which harmful for network because the main aim of attackers tries to disturb the network performance like congestion, propagation of fake route information or modification or disruption etc. Warm hole attacks & black hole attacks are the examples of these attacks [11].

Passive Attacks: This is the type of attacks in which extract the important information without modify or change the data packet in the network, this means attacker act as the intermediate node does not harm the network but only take the valuable information or knows about which type of communication are going on (between sender & receiver).Eavesdropping, traffic analysis, traffic monitoring and snooping are the examples of passive attacks [11][9].

Know we further discuss various types of routing attacks as following:

2.1 Black Hole Attack

It is type of active attack. Attacker act as malicious node in the network. Firstly, malicious node able to enter between the genuine communicating nodes in the network. It uses the packet information which passes between source to destination for wrong purpose or discard the packet. Malicious node provides fake routing information to other nodes or also changes the destination address of the

packets passing through them because it advertising itself having shortest path to the source node, so this attack also know as packet drop attack and stops the forwarding of data packet to next hop[7][6]. Black hole attack further into two types as following:

a) Single black hole attack: it is type of black hole attack in which only single node act as malicious nodes which carry out the attack on operation, discard the data packet. So it is known as single black hole attack [7].

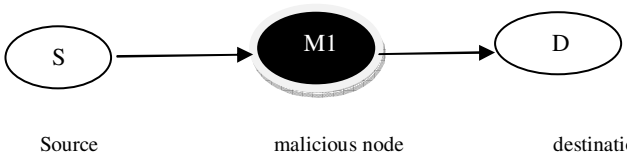

Fig.2 Single black hole attack

b) Cooperative black hole attack: It is second type of black hole attack in which two or more malicious nodes work together to carry out the attack on operation. It is more complex or damaging rather than the single black hole attack. In the following diagram, M1, M2, M3 are the malicious nodes & S act as source node & D act as a destination node [7].

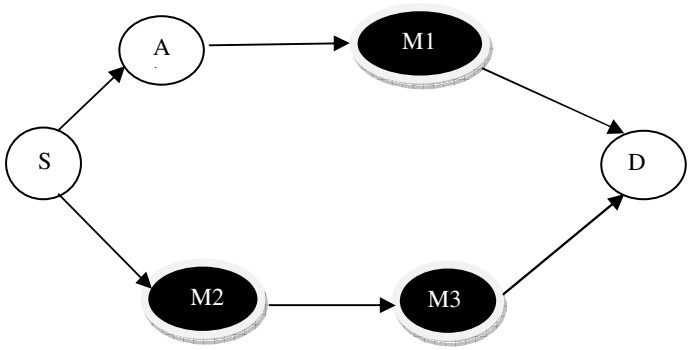

Fig.3 Cooperative black hole attack

2.2 Flooding Attack

This attack is the type of denial of service (dos) attack because when the normal communication are carry on between source & destination, suddenly malicious nodes may also insert fake packets into the network which forwarding the huge unnecessary packets to the targeted node . Due to this, the targeted node will be flooded known as flooder node unable to send or receive any data packet & floods the whole network. So this attack creates many issues like consume the power in term of battery power & bandwidth, regarding network performance and reduces the throughput of network [6][12]. This attack is further divided into three types as following:

a) RREQ Flooding: In this type of flooding attack, attacker node broadcast various RREQ packets for the node which may exist or not exist in the network. For this purpose, the attacker deactivates the RREQ rate so it will consume network bandwidth [12].

b) Data Flooding: In this type of attack, malicious node used huge amount of data packets to flood the whole network or builds a path to all the nodes, so that fake data packets sends to the genuine nodes & fail the network resources. It will be hard to detect [12].

c) SYN Flooding: Due to this type of attack, large amount of memory consumed because attacker node sends the number of synchronization packets to the destination node [12].

2.3 Grey Hole Attack

This attack simply variation of black hole attack initiate in Adhoc network in which malicious node drop certain selective packets or some forward to the nodes. In this attack, sometime a node may behave maliciously but behaves normal node later on. We can say that, this attack act as slow poison in the network & cannot suppose how much data can be lost. Gray hole node are very effective in Manets [2][4][5].

2.4 Warm Hole Attack

This is serious type threat in wireless network. In this attack, two malicious nodes are used to make a tunnel between them. Tunneling is called warm hole because one malicious node receives the packet from one at the end & tunnel them to another location& retransmits packets in the network. So this attack is also known as tunneling attack. Normal nodes supposed malicious nodes as a neighbor node, in this way they compromised with malicious nodes which create a shortcut path in the network for communication between the nodes but it cause issues like packet drop, listening of confidential information between the nodes, alteration of transferred data packets[8][11][1].

2.5 Sink Hole Attack

This attack is harmful & risky attack in Manets. In this attack, sinkhole nodes create a fake routing way or act as specific node to attract the neighbor nodes & receive whole network traffic. This attack also create many issues like modify the data packets or drop them silently, increase network overhead, decreases network life time and at the end may destroy the network[10].

3. Conclusions

In this paper, we have overview on concept of Manets, but there are many security threats also created problem in the performance of network. So we have focus on various types of routing attacks in Manets like black hole attack, flooding attack, gray hole attack, warm hole attack and sinkhole attack which effects on network performance like throughput, packet delay ratio, congestion etc. No doubt a lot of works are done on detection & prevention of these various attacks but these are big challenging threats in Manets .

References

[1] Kathole A.B., Pardak he N.V., Kute D.S. & Patil A.S,, "A review paper on comparison and analysis of different attack and intrusion detection system" International Journal of Cryptography and Security, Volume 2, Issue 1, 2012

[2] Maulik H. Davda, Sheikh R.Javid,, "A Review Paper on the Study of Attacks in MANET with Its Detection & Mitigation Schemes" International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 4, April 2014

[3] Akansha Shrivastava and Rajni Dubey,, "Wormhole Attack in Mobile Ad-hoc Network: A Survey" International Journal of Security and Its Applications Vol.9, No.7, 2015

[4] Shani Makwana, Krunal Vaghela,, "Cooperative Gray Hole Attack Detection and Prevention Techniques in MANET: Review" International Journal of Science and Research, Volume 4 Issue 1, January 2015

[5] Ashok Desai,, "Review Paper on Detection and Prevention Techniques of Gray-Hole Attack in Manet" International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 5, May 2013, pg.105 –108

[6] Ruchita Meher, Seema Ladhe,, "Review Paper on Flooding Attack in MANET" Int. Journal of Engineering Research and Applications,ISSN : 2248-9622, Vol. 4, Issue 1, January 2014

[7] Ravinder Kaur, Jyoti Kalra,, "A Review Paper on Detection and Prevention of Black hole in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6,June 2014

[8] Aarti Chauhan, Puneet Rani,, "A Detail Review of Routing Attacks in Mobile Ad Hoc Networks" International Journal Of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015

[9] S. Anusuya, Dr. S.Meenakshi,, "A Review of Routing Protocols and Attacks in Mobile Ad-hoc Network" International Journal of Advanced Research in Computer Engineering & Technology Volume 4 Issue 9, September 2015

[10] Gagandeep, Aashima, Pawan Kumar,, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 –8958, Volume-1, Issue-5, June 2012

[11] Kaur Sharndeep, Gupta Anuj,, "A review on different secure routing protocols and security attacks in mobile ad hoc networks" International Journal of Advanced Engineering Technology, Vol. V/Issue IV/Oct.-Dec.,2014

[12] Shruti Bhalodiya, Krunal Vaghela,, "Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol" International Journal of Computer Application, Volume 125 –No.4, September 2015

Author Profile:

Navpreet kaur is currently in the final year of degree course of Master's of engineering and technology from Sri Sai College of Engineering and Technology, Manawala, , Amritsar under I.K. Gujral Punjab Technical University, Jalandhar

Prof. Puneet Kumar the guide and assistant professor in Sri Sai College of Engineering and Technology , Manawala , Amritsar under I.K. Gujral Punjab Technical University, Jalandhar