A Review paper on study of collaborative attack on Mobile ADHOC network in MANET

1Gurpreet Kaur, 2 Deepinder Kaur Dhaliwal, 3 Neha Soni
1,3CSE Dept, DESH Bhagat University MandiGobindgarh,Punjab , India
2AP(CSE Dep)t,,DESH Bhagat University MandiGobindgarh,Punjab , India
ruheesoni@yahoo.co.in

Abstract: **Wireless networks are become more popular now days because of the increase in the demand of wireless network by the users. In a manet there a no of attack wireless network. In such a way collaborative attack is a security threat or an active type of attack in which the malicious nodes can read the data packets falsely claiming the fresh route these can nodes reads the various routing protocols for having the path from source to destination.in this review paper we can review the various attacks like wormhole attack on manet.**

Keywords: **manet, wormhole, blackhole, multiple nodes, collaborative attack.**

I. Introduction

Network of ADHOC is also called as IBSS (i.e Independent basic set station) In a ad hoc network nodes cannot have any access point .nodes can communicate with each other directly. Due to the presence of nodes Ad hoc network is being called as MANET. (Mobile Adhoc network). MANET is defined as a group of nodes which are self managed and communicate with each other directly. MANETs contains a dynamic topology in which nodes can easily join and leave the network at any time. MANET is suitable for both the wired and wireless network infrastructure. In a MANET there is no centralized authority so security is a great issue in this. Presence of various wireless links also cause a complex issue in a security of a MANET, another feature of MANET is moderate bandwidth, limited battery power. There are a various attacks present in a network but when two attacks are simultaneously occurred called as a collaborative attack.

II. Collaborative attacks

Due to presence of group of nodes in a MANET the network works as without centralized administration.

The classification of the attack can be done as active attack, passive attack. There are two sources of attack i.e internal and external. Collaborative attack is defined as the Homogeneous attack: when a single attack is occurred in MANET is known as Homogeneous attack. Attack i.e black hole, wormhole attack. Collaborative attack: whenever multiple attacks are occurred simultaneously on a two different malicious nodes is known as collaborative attack.

III. Various attacks are

1) DOS attack: Denial of service attack is the type of active type attack. DOS attack is also known as the distributed denial of service attack and it makes the resources become unavailable to its intended users. Analysis of traffic: The data packets and the traffic pattern are important for adversaries For example, confidential network information of topology can be formed by evaluating traffic patterns. By destroying the nodes traffic analysis is also known as active attack that can stimulates self-organization in the network, and topology can be gathered the valuable data.
2) Snooping Attack: Snooping is also known as an unauthorized access to data. It is similar to eavesdropping but the limited to gaining access to data is not necessary during transmission. Snooping can include casual observance of an data that can appears on another's computer or watching what someone else is typing. In snooping the software programs to remotely control the computer.
3) Active attack: In a Active attack, the intruder performs an violation on either the network resources or the data transmitted; this can be done by IJNC (i.e International Journal of New Computer Architectures) and Their Applications causing routing disruption, network resource degradation, and breakage of nodes. These following are the types of active attacks over MANET and how the attacker's threat can be performed
4) Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and may be anode's resources consumed, such as battery power or to disrupt the routing and computational operation to cause severe degradation in network performance [7].
5) Black hole Attack: Route discovery process in AODV is vulnerable to the black hole attack [7]. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough route of data transmission, It devised to reduce routing delay, is used by the malicious node to compromise the system. Black hole attack is a type of attack which a drop the data packet .Black hole attack is a special type of attack which can attract all the nodes and drops the data packets. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.[10]

6) Gray hole attack: Gray hole attack is a attack is also called as a routing misbehavior attack which leads to dropping of messages. The gray hole attack can be categorized in two phases. In the first phase the node advertise itself as having a valid route to destination and in phase second, nodes intercepted packets drop with a certain probability [8]. In this kind of attack the attacker misleads the network by approving to forward the packets in the network. As soon as it receive the packets from the neighboring It node, the attacker falls the packets, this attack comes under the category of active attack. In the beginning the attacker nodes behaves casually and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets are starts dropping the packets and it can launch DoS i.e denial of service attack. The malicious activities of gray hole attack may be different from time to time. It may drops packets while forwarding them in the network. In some other attacks the attacker node behaves maliciously for the time until the packets are dropped and then nodes are shown their normal behavior. Due this behavior it is very tricky for the network to figure out such kind of attack.

7). Wormhole attack: there are a various types of attack on MANET but wormhole attack is a special type of attack because in this attack malicious nodes cannot drop the packet but it creates a different kind of path to reach the data packets at destinations.

IV. Types of attack

There is another we classified the collaborative attack into two categories these are:

1) Single attack: whenever only single node act as a malicious node then it act as a single wormhole attack.
2) Collaborative attack: when two or multiple nodes are act as malicious nodes then it is called as wormhole attack with multiple malicious nodes or collaborative attack.

V. Categorization of collaborative attack

In the collaborative attack there are large numbers of nodes are involved .the existence of these nodes may be physical or not .In this paper we are study the various types of attack on the basis of collaborative attack we are categorize it as following categories these are as:

a) Direct collaborative Attack: In an original network the nodes are also present in a network. And the malicious nodes are joining the network. This type of collaborative attack is known as a direct collaborative Attack. The black hole Attack and wormhole Attack is also comes under these categories.
b) Indirect collaborative Attack: In this type of Attack the different non existence nodes are responsible for redirect the data packets to the malicious nodes which are fake. This type of collaborative attack is known as an Indirect Collaborative Attack.

VI. Routing protocol description:

1) Table driven: Table driven routing protocol is maintains the fresh lists of destinations and the routes of the nodes. It has a large capacity to keep the information current and a lot of routing protocol may not be used. The main disadvantages of this routing protocol are that slow reaction on restructuring and failure. Table driven routing protocol is also known as proactive routing protocol.
2) On demand routing protocol: On demand routing protocols are the reactive routing protocol. On demand routing protocol are find the route on demand by flooding network with route request packets. The main disadvantage of this routing protocol is that excessive flooding can lead to network clogging. It cannot be appropriate for the real time communication.
3) Hybrid routing protocol: Hybrid routing protocol can be defined as the combination of advantages of the both routing protocols i.e proactive (OLSR Optimized link state Routing)) and reactive (Ad-hoc on Demand Vector) routing protocols .example of the hybrid routing protocol is ZRP (zone routing protocol).

VII. There are various security issues

Decentralized network topology: In a MANET nodes are freely moves and communicate with each other and easily leave and join the network which may results in changes in routes and there may nodes can loss their packets.

Decentralized monitoring: MANET can contain the wired and wireless infrastructure .so due to lack of centralization there may occur the number of attacks in a network.

Cooperative algorithms: there is a need of trust between the neighboring nodes in routing algorithms.

Bandwidth constraint: In a MANET wired infrastructure has need of more power than the wireless links infrastructure.

Limited physical security: changes in the nodes results in the higher security threats and it may increases the possibility of attacks.

Energy constrained operation: it means that ad hoc network have a limited power and storage capacity.

VIII. Scope and Aim

on the basis of the features related to the MANETs there are causing the numbers of the problems in such networks .our research on MANET are to be related to focuse on the number of attacks either single attack or multiple attack.

There are a number of attacks but we categorize the wormhole attack and Black Hole attack and we implement that attacks and observe the impact of collaborative attacks.

IX. Conclusion

In this paper we are to implement the Black Hole attack and wormhole attack as a collaborative attack on MANET. We are also evaluating the performance evaluation of MANET with collaborative attack and without collaborative attack and we also prevent the collaborative attack on MANET.

Related work: we are discus the various types of attack in paper. In future there are a large number of work has been pending in detection techniques. And we use another kind of attacks to implement on MANET.

References

1. A comparative study of collaborative attack on mobile adhoc networks, international journal of engineering and technology and advanced engineering, august2014.
2. A review on wormhole attacks in MANET ,journal of theoretical and aplled information and technology,september2015.
3. performance evaluation of collaborative attacks in MANET, international journal of computer science and mobile computing ,july 2014.4. A review on black hole attack in MANET, International journal of engineering research and applications, June 2012.
5. Wormhole Attack Detection Technique in Mobile Ad Hoc Networks, *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, October 2014.
6.A Study on Wormhole Attacks in MANET , International Journal of Computer Information Systems and Industrial Management Applications, ISSN 2150-7988 Volume 3 (2011) pp. 271-279 .
7. Survey on Routing Protocols on Mobile Adhoc Networks , 978-1-4673-5090-7/13/$31.00 ©2013 IEEE
8. Analysis And Evaluation Optimization Dynamic Source Routing (DSR) Protocol in Mobile Adhoc Network Based on Ant Algorithm.IEEE
9. A Review of Blackhole Attack in Mobile Adhoc Network , 2013 IEEE.
10. Performance Analysis of Various Routing Protocols (Proactive and Reactive) for Random Mobility Models of Adhoc Networks, 2012 IEEE.
11. Relative Cluster entropy based Wormhole Detection using AOMDV in Adhoc Network , 2012 Fourth International Conference on Computational Intelligence and Communication Networks.
12. Mohamed Amnai, Youssef Fakhri, Jaafar Abouchabaka "Throughput-Delay Optimisation with Adaptive Method in Wireless Ad Hoc Network" IEEE 2010, 5th International symposium on Communications and Mobile Networks(ISVC)ISBN: 978-1-4244-5996-4.
13. Krishna Gorantala, "Routing Protocols in Mobile Ad hoc Networks" Master Thesis in Computing Science, Umea University, June 15,2006.
14. K. Maheswari, M. Punithavalli. "Performance Evaluation of Packet Loss Replacement using Repetititon Technique in VoIP Streams", *International Journal of Computer Information Systems and Industrial Management Applications*, 2, pp. 289-296, 2010.
15. M. Rajput, P. Khatri, A. Shastri, K. Solanki. "Comparison of Ad-hoc Reactive Routing Protocols using OPNET Modeler". In *Proceedings of International Conference on Computer Information Systems and Industrial Management Applications*, pp. 7-12, 2010
16. R.H. Khokhar, Md. A.Ngadi, S. Manda. "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Science and Security*, 2 (3), pp. 18-29, 2

