Single and Cooperative Black Hole Attacks in MANET

[1]Karthick M. , [2]Sakthivel D.
Research Scholar, Assistant Professor,
Dept. of CSE, Sree Saraswathi Thyagraja collge(Autonomous), Pollachi, Tamilnadu.

Abstract - Malicious nodes attacks are the vital problem in the mobile ad-hoc networks. It leads to loss of packets, reduce the throughput and increase the end to end delay during the transmission. Single or cooperative black hole attacks are the one kind attack to degrade the performance. This survey paper analyse the single and cooperative black hole attacks and existing research works performed in the detection and avoidance of black hole attacks inAODV and DSR protocols in the MANET.

Index Terms - single black hole, cooperative black hole attack, AODV and DSR

I. INTRODUCTION

Wireless mobile ad hoc networks are dynamically changed and self-configuring network with freely movable nodes. Ad hoc is Latin and means "for this purpose". Each device in mobile ad hoc networks is free to move independently in all directions, and will therefore change its links to other devices frequently. Setting up of fixed access points and backbone infrastructure is not always viable Infrastructure may not be present in a disaster area or war zone. Infrastructure may not be practical for short-range radios; Bluetooth (range ~ 10m).

The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Dynamic Source Routing [DSR] and AODV are some algorithms that have been designed to handle such transmission of data.

Fig.1. Infrastructure of MANET

Mobile ad hoc networks mainly used in the fields of medical emergency, natural disasters, military and secured communication areas. In these applications, all the nodes of the mobile ad hoc network belong to a single authority and have a common goal. With the progress of technology, it has now become possible to deploy mobile ad hoc networks for civilian applications as well.

The mobile ad hoc network is an integration of more than one wireless nodes and have the capacity of transferring data to one another without any kind of help from a centralized administrator. Every device acts as a router and end system in ad hoc network. The network topology in a wireless ad hoc network is dynamic due to the integration of the nodes changing with time because of the mobility of nodes, entry of new nodes and flight of nodes.

Ad hoc nodes are devices to have the capacity to identify the existence of other such devices in order to permit data sharing and communication. Besides that, it ought to additionally have the capacity to distinguish type of relating attributes and services. Due to the mobility of nodes the amount of wireless nodes will change, routing data additionally changes to follow changes in the connectivity of links. Henceforth, the topology of the network is a great deal are dynamic and the adjustments are frequently unusual as contrasted with the settled type of actual wired networks.

Wireless network technology allows as accessing information, services or resources from remote place electronically from everywhere. It becomes tremendously popular due to its usage and wide range of applications. The revolution in wireless communication is bringing fundamental changes to data networking, telecommunication and is making communications and networking anytime, anywhere possible. A set of nodes may be compromised in such a way that it may not be possible to detect their malicious behaviour easily. Malicious nodes can generate new routing messages to advertise non-existent links and provide incorrect link state information, and flood other nodes with routing traffic. One of the widely known attacks is the Black Hole Attack.

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbours. A single black hole attack is easily happened in the mobile ad hoc networks [1].

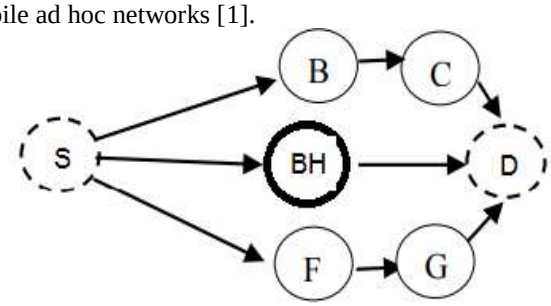

Fig.2. Single Black Hole

The cooperative black hole is a type of attack in which black hole nodes act in a group together [1]. For example when multiple black hole nodes are acting in coordination with each other, the first black hole node refers to the one of its teammate in the next hop .This type of attack harms the system very much and affect the throughput of the system.

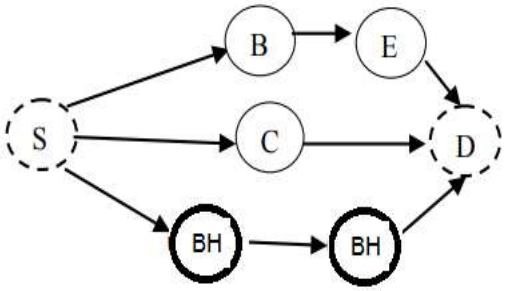

Fig.3. Cooperative Black Hole

II. REVIEW OF LITERATURE

Rajesh Sharma et al. proposed a reputation method based solution to resolve the routing issued in the MANET generated by the misbehaving nodes [2].

Sohail Abbas et al. classify their active and passive acknowledgment monitoring techniques in mobile ad hoc networks selfish or misbehaving nodes can disrupt the whole network and severely degrade network performance [3].

RenuDalal et al. provide the different ways to achieve trust in mobile Ad-hoc Network. Providing the safe communication between mobile nodes, reorganization the position of nodes, reducing overhead are more complicated issues in the mobile ad-hoc networks. So providing trust schemes is an important in this network [4].

Santhosh Krishna B. Vet et al. focus on single and multiple black hole attacks in the mobile adhoc networks. The implementation shows black hole nodes includes active routing misbehaviour in DSR protocol [5].

Isaac Woungang et al. introduced new scheme for detecting black hole nodes and its attacks. Before the actual routing mechanism, this new scheme sends the fake route request packets to all nodes and identifies the malicious nodes. [6].

Poonam K Gar et al. They had discussed and proposed a new algorithm to find route to the destination as a weighted average of the trust value of the nodes in the route, with respect to its behaviour observed by its neighbouring nodes and the number of nodes in the route is calculated [7].

SangheetaaSukumran et al.[8] proposed a solution for on-demand routing protocol using calculating reputation values for each nodes mechanism. Any node is supposed to maintain a good reputation value in order to receive network services. When a node tries to identify a route, its route request will be forwarded by the neighbouring nodes only if it reputation value is higher than the threshold value i.e. this node must be in the white list. Thus each noderequiresmaintaining a virtuous reputation value to stay with the services. A misbehaving node which is isolated has no chance of re-joining the network until the entire network is reformed. It degrades the network efficiency, low reputation value nodes are not allowed to utilize the services in the network.The authors provided a cache clearance for each node in the network to reduce the network overhead, it helps to allow low reputation nodes to utilize the services. It helps to improve the efficiency of the network.

A formal study of MANET Security issues are presented by Nishu et al [9] which says MANET pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and limited resource constraints etc. Security is not a single layer issue but a multi-layered issue. The Study of this important issue reveals that security is divided into different directions of the work like secure routing, key exchange, distribution and management, secure architecture, intrusion detection and protection etc. They considered the problem of incorporating security mechanisms into routing protocols for ad hoc networks. Canned security solutions like IPsec are not applicable here. They looked at AODV in detail and developed a security mechanism to protect its routing information by developing a technique to periodically discover shortcuts to the active routes that can be used with any destination vector routing protocol

Khalid at el [10] investigated some very common but challenging issues experienced by ad-hoc wireless communication. They have divided their studies into three sub-domains i.e. Security Models, Vulnerability in Current Protocols and Attacks. They Considered Security attacks as major issue of ad hoc networks which can be overcome up-to a level by adopting some proposed schemes. They explored the proposed methodologies and security schemes that guard against large

number of attacks including DOS, Wormhole, Black hole and Flooding attacks. And concluded that these schemes are effective for detection attacks but still have limitations which raise questions on their usability. The protocols associated with MANETs require more research; especially reactive protocols may be trapped by intruders at the time of route discovery process.

Weber et al [11] have studied and simulated different sensors that can detect different kinds of selfish nodes. They also proposed Mobile Intrusion Detection System (MobIDS) with a good confidence to detect selfish nodes. If multiple sensors are active in parallel and a selfish node is detected by a number of these sensors, then this is a good indication for excluding the node from the network. One remaining problem with their current simulations is that all thresholds need to be set manually in order to get good detection results.

In this paper [12] a performance simulation has been done on AODV protocol in NS-3 and concluded that due to the presence of selfish nodes in the network, the average percentage of packet loss in the network increases, thus decreasing the overall network throughput. Therefore both data packets and routing control packets need to be secured from the selfish nodes.

Another Research work carried out by Mohammad al-Shurman et al [13] they simulated black hole attack in AODV protocol and presented two possible solutions are find the more than one route from the source to destination and second one is include the packet sequence number for each packet.

III. CONCLUSION AND FUTURE WORK

This surveydiscloses that the single or cooperative black hole attack is the critical threat and identifies the weaknesses in packet delivery, routing overhead and end-to-end delay. Various techniques and approaches are observed in this study to detect the single or cooperative black hole nodes. After studying all the approaches examines that the most of the approaches has low packet delivery ratio and also high overhead. In future work, develop such approach which can efficiently minimize all these constraints.

REFERENCES

[1] MamtaSengar, PawanPrakash Singh, SavitaShiwani, “Detection of Black Hole Attack In MANET Using FBC Technique”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 2, March – April 2013 ISSN 2278-6856.

[2] Rajesh Sharma &SeemaSabharwal “Dynamic Source Routing Protocol (DSR)”, IJARCSSE, Volume 3, Issue 7, July 2013 pp. 239-241.

[3] Sohail Abbas, MadjidMerabti, and David Llewellyn-Jones “A Survey of Reputation Based Schemes for MANET” 2010.

[4] Renu Dalal1, ManjuKhari and Yudhvir Singh “Different Ways to Achieve Trust in MANET” International Journal on Ad Hoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.

[5] Santhosh Krishna B.V, Mrs.Vallikannu A.L “Detecting Malicious Nodes for Secure Routing in MANETS Using Reputation Based Mechanism” International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010.

[6] Isaac Woungang, Sanjay Kumar Dhurandher, RajenderDheerajPeddi and Mohammad S. Obaidat, Fellow of IEEE and “Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks”, 2012

[7] Poonam, K. Garg, M. Misra “Trust Based Multi Path DSR Protocol”, International Conference on Availability, Reliability and Security IEEE 2010.

[8] SangheetaaSukumran, VenkateshJaganathan, ArunKorath “Reputation based Dynamic Source Routing Protocol for MANET” International Journal of Computer Applications (0975 – 888) Volume 47– No.4, June 2012

[9] NishuGarg, R.P.Mahapatra, “MANET Security Issues”, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009 .

[10] KashifLaeeq, Khalid Khan, “Performance Study of Approaches for Detecting Attacks in Ad Hoc Wireless Networks”, JOURNAL OF COMPUTING, VOLUME 3, ISSUE 2, FEBRUARY 2011, ISSN 2151-9617.

[11] F. Kargl, A. Klenk, M. Weber, and S. Schlott, "Sensors for Detection of Misbehaving Nodes in MANETs", in Proc. DIMVA, 2004, pp.83-97.

[12] SatyanarayanaVuppala, AlokparnaBandyopadhyay, PrasenjitChoudhury and Tanmay De, “A Simulation Analysis of Node Selfishness in MANET using NS-3”, Int. J. of Recent Trends in Engineering and Technology, Vol. 4, No. 1, Nov 2010.

[13] Mohammad Al-Shurman, Seong-Moo Yoo, Seungjin Park, “Black Hole Attack in Mobile Ad Hoc Networks”, Proceeding of 42nd Annual Southeast Regional Conference ACM-SE 42, Publisher ACM Press, April 2004.