www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 8 Aug 2015, Page No. 13717-13721

A Survey on Detection and Prevention of Black Hole & Gray hole attack in MANET

***Monika*[1], *Swati Gupta*[2]**
[1]M.Tech Scholar,Geeta Institute of Management and Technology, Kurukshetra

monikamuradia@gmail.com

[2]Astt.Professor,Geeta Institute of Management and Technology, Kurukshetra

missbhasin@gmail.com

Abstract: ***A mobile ad-hoc network (MANET) infrastructure less dynamic network consists of collection of wireless mobile node that communicates with each other without the use of centralized network. Security in MANET is the most important concern for the basic functionality of network. The malicious node falsely advertises the shortest path to the destination node during the route discovery process by forging the sequence number and hop count of routing message . In this paper ,we have discussed various techniques of detection and avoidance of Black hole and gray hole nodes in MANET .***

Keyword : MANET , AODV Protocol ,Black Hole Attack , Gray Hole attack , Digital Signature Technique.

I.INTRODUCTION

In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized .Due to absence of any kind fixed infrastructure and open wireless medium security implementation is difficult. In Manet each node functions as a host as well as router, forwarding packets for another node in the network. MANET is vulnerable to various kinds of attacks. These include active route interfering, imprecation and denial of service. Black hole attack is one of many possible attacks in MANET. In this attack, a malicious node sends a forged Route REPLY (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. The malicious node launches this attack by advertising fresh route with least hop count and highest destination sequence number to the node which starts the route discovery .

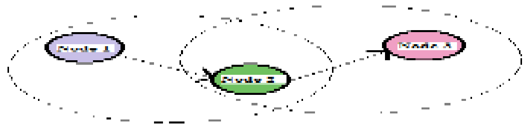

Fig 1: Route discovery process

Routing Protocol in MANET

1. Proactive Routing Protocol-Here the mobile nodes periodically exchange routing information and maintain the network topology information in routing table. It is also called table driven routing protocol.

2. Reactive Routing Protocol- Here there is no exchange of routing information periodically. Instead a necessary path is obtained when required. it is also called on demand routing protocol.

3. Hybrid Routing Protocol- It combines the features of both proactive and reactive routing protocols. A table driven approach is used within the routing zone of each node while an on demand approach is used for the nodes that are outside the routing zone.

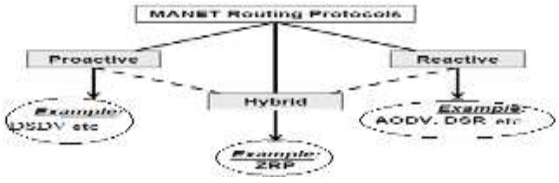

Fig 2 : Routing Protocol

II. AODV Protocol

The Ad-hoc on demand distance vector routing protocol is one of the widely used routing protocols in MANET. The route is established only when it is desired by the source node for data packets. Whenever node requires a route to the destination, a route discovery process is initiated. The source node floods the Route Request packet to its neighbours. The Route Request packet contains source identifier, destination identifier, source sequence number, destination sequence number, broadcast ID and TTL (Time to live). The intermediate node either forwards the packet or prepares a Route Reply if it has a fresh or valid route to the destination. This validity is determined by comparing the sequence number of intermediate node with the destination sequence number of Route Request packet. The destination node or the intermediate node that has the freshest route sends the Route Reply message back to the source node in the reverse path.

2). The source node receives many Route Reply packets and the fresher and shorter path is selected to send the data packet.

III .Classification of Security attacks :

1) Passive attacks:

A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic.

2). Active attacks:

Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorised access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc.

Attacks at Physical Layer:

Some of the attacks identified at physical layer include eavesdropping, interference, and jamming etc.

1) Eavesdropping:

It can also be defined as interception and reading of messages and conversations by unintended receivers. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication.

2) Jamming:

Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. Jamming attacks also prevents the reception of legitimate packets.

3) Active Interference*:* An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications.

Attacks at Data link layer

The data link layer can classified attacks as to what effect it has on the state of the network as a whole .

1) Selfish Misbehaviour of Nodes:

The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources and to conserve of battery power.

2) Malicious Behaviour of nodes:

The main task of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighbouring nodes. Attacks of such type are fall into following categories.

3) Denial of Service (DoS):

The prevention of authorized access to resources or the delaying of time-critical operations. A denial of service (DoS) attack is characterized by an attempt by an attacker to prevent legitimate users of a service from using the desired resources and attempts to "flood" a network, thereby preventing legitimate network traffic.

Attacks at Network Layer:

1. Black Hole attack

The Black hole attack in MANET is very serious problem. It affect the security in MANET .During the route discovery process it shows the highest destination sequence number . It shows the shortest path towards the destination. Source node will select this shortest path from this node towards destination . Then source node will send the packet to this node . It will drop or consume that packet and don't allow to forward towards next node . As the result of this , Packet delivery ratio , Throughput , end to end delivery ratio will decrease . In this paper ,to avoid this defect I have tried to detect then prevent this defect using digital signature techniques .

Single Black Hole Attack :

AODV route discovery mechanism is based on RREQ/RREP messages. Source node broadcasts the RREQ message to its neighbors. Either the destination or intermediate node sends RREP. The RREP received first by source node is accepted and all further RREPs are discarded. Black hole node takes benefit of this feature of AODV and sends RREP first even without checking its routing table. In this way, a route through black hole node is setup and black hole node consumes all the forwarded packets

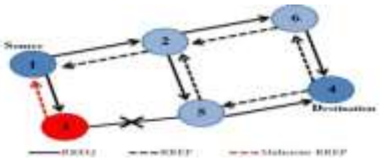

Fig 3: Single Black Hole Attack

In figure ,node 3 is black hole node through which final route is established. Being the black hole node, it consumes all the packets without forwarding them.

2. Cooperative Black Hole Attack

Cooperative Black hole means the malicious nodes act in a group . As an example,

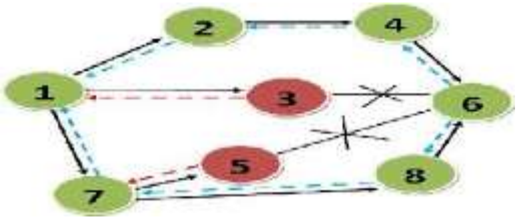

Fig 4: cooperative black hole attack

In above Example, when multiple black hole nodes are acting in coordination with each other, the first black hole node 3 refers to one of its teammates node 5 as the next hop, .The source node 1 sends a “Further Request (FRq)” to 5 through a different route (1-7-node 5) other than via 3. Node 1 asks node 5 if it has a route to destination node 6. Because node 5 is cooperating with node 3, its “Further Reply (FRp)” will be “yes” to both the questions, then all the packets are consumed by node 3 and don’t allow it to further proceed.

3. Gray Hole attack

Gray Hole attack is a variation of the black hole attack in which the malicious node may behave as an honest node first during the route discovery process and then may change its state to malicious and vice versa. This malicious node may then drop all or some of the data packets. The gray hole attack is difficult to detect due to congestion, overload and also due to malicious nature and ability of changing states. Instead it behaves as an honest node and when data packets arrive through this path, it drops all the data packets. A condition is added to drop all the data packets if it is not the destination otherwise receive all the data packets. Gray hole node act honest node during route discovery process but in actual it is an attacker .

• Dropping all UDP packets while forwarding TCP packets.

• Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures .

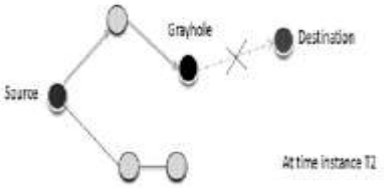

Fig 5: Gray Hole Attack

IV. Literature Review:-

There are several techniques used for the detection prevention of malicious node in manet .

1. Pradeep Kumar Sharma et al, proposed a centralized system with MANET then it prevent the attacks. It is a type of network where all users get connected to a main server which plys role of important agent for all transmissions and receptions. The server acts like a database for storing information about the users and all the communications occurring between the nodes. Instant message sending and receiving require main server-structure like these. Also called centralized server-structure. Black Hole attacks are more vulnerable than Gray Hole attacks because the packet drop ratio is high for Black Hole attacks compared to Gray Hole attacks, not only that the normalized routing load also increases in the presence of Black Hole attacks compared to Gray Hole attacks.

2.Chander Diwaker, Sunita Choudhary, proposed a technique of identifying and isolating black hole attack by eradicating the disadvantages of DBA-DSR algorithm. DBA-DSR is enhanced version of DSR protocol and detects malicious nodes with aid of fake Route request and Route Reply packet. This invites several disadvantages of this method, the main implies increased overhead packets due to sending of acknowledgement packets repeatedly to keep an eye on fake route reply packets generated from malicious nodes.

3.Ravinder kaur , Jyoti kalra proposed a techniques that is Digital signature , to detect the malicious node in network digital signatures are used. Digital signature is the one of the verification technique. All nodes have legitimate digital signature. id will be verify . If it is listed in node list then it is OK , it is a valid node else malicious node .

4. Suparna Biswas, Tanumoy Nag , Sarmistha Neogy proposed a solution for detecting and avoiding black hole attacks (both single and cooperative) and ensuring secure packet transmission along with efficient resource utilization of mobile hosts at the same time. According to our proposal, evaluation of trust of every node in the network is based on parameters such as stability of a node defined by its mobility and pause time, remaining battery power etc. This trust of a node forms the basis of selection of the most reliable route for transmission. The simulation results show that our solution provides good performance in terms of throughput, secure routing, and efficient resource utilization.

5.Harsh Pratap Singh, Virendra Pal Singh,Rashmi Singh ,a review on a various types of coordinated attack is deliberated such as blackhole / grayhole attack which are most serious threats in mobile ad hoc network. In cooperative blackhole attack more than one node collude to each other hence this attack is more challenging to identify. This paper presents a review of different security mechanism to eliminate the blackhole / grayhole attack from the network.

6. Sandeep Kumar , Mrs. Sangeeta ,They proposed a different techniques to prevent a gray hole attack in MANET.Neighborhood-based and Routing Recovery Scheme , Using watchdog/pathrater Scheme, Counter-Threshold Based & Query- Based Scheme, Aggregate

signature algorithm , Centralized intrusion detection scheme based on Support Vector Machines, Cross layer intrusion detection architecture based scheme, Channel appraised method .

7. Alka Chaudhary, V.N. Tiwari proposed A Reliable Solution against Packet Dropping Attack due to Malicious Nodes Using Fuzzy Logic in MANETs they develop intrusion detection system using fuzzy Logic to detect the packet dropping attack from the mobile ad hoc networks and also remove the malicious nodes in order to save theresources of mobile nodes. For the implementation point of view Qualnet simulator 6.1 and Mamdani fuzzy inference system are used to analyze the results. Simulation results show that our system is more capable to detect the dropping attacks with high positive rate and low false positive.

8.Jitendra Parmar , Jitendra Parmar proposed a Different Approach of Intrusion Detection and Response System for Relational Databases . detection of intrusion is detected that are possible in the databases and various authentication techniques are implemented to made this databases secure. Database security and authentication such as 3 factor authentication, intrusion response system, timestamp, triggers such factors provides more security to the database. The proposed methodology implemented here provides security,
authentication, and database pol**icies.**

9. Cansin Turguner , Secure Data Dissemination in MANETs by means of Mobile Agents in this paper it is coped with many security issues such as unauthorized attempts, security threats and reliability. Using mobile agents in having low level fault tolerant ad-hoc networks provides fault masking that the users never notice. Mobile agent migration among nodes, choosing an alternative
path autonomously and, having high level fault tolerance provides more reliable networks, which have low bandwidth and high failure ratio..

10. Changhui et al proposed method that provide a scheme that with hash based message authentication code to overcome the shortcomings. Hash based message authentication code using cryptographic hash functionsuch as SHA-1 in combination with secret key.It provides the integrity of information transmitted over a unreliable mediun based on secret key. In this method HMAC checking and symmetric ecryption used to replace complicated ECC to achieve secure communication.

11.M.A.Matin et al proposed a method on symmetric encryption technique with AES algorithm in MANET and WLAN. Symmetric encryption is faster and requires less computational processing time. The increase in key size as well as block size, the security gets enhanced and linear cryptanalysis and differential cryptanalysis require more time to break the proposed cipher here.

12. Uttam Ghosh et al proposed a ID based distributed dynamic IP configuration scheme for address allocation. They discussed the three categories namely best effort allocation, Leader based allocation and Decentralized allocation. And gave solution to overcome the problems arised by these three categories. For address detection they denied the concept of DAD scheme.

V. Conclusion and Future Scope :

Various methods have been studied in literature review used for detection and prevention of black hole and Gray hole . There may be many other methods too **,** by which we can prevent malicious node and increase packet delivery ratio , end to end delivery, reduce the dropping of packet and increase throughput of the system. In future we will enhance the performance and increase the packet delivery ratio more .

REFERENCES

[1] D. Djenouri, L. Khelladi and N. Badache, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," IEEE Commun. Surveys and Tutorials, vol. 7, no. 4, pp. 2-28, 2005.

[2] S. Desilva, and R. V. Boppana, “Mitigating Malicious Control Packet Floods in Ad Hoc Networks,” Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[3] M. G. Zapata, "Secure Ad Hoc on-demand Distance Vector (SAODV) Routing," IETF Internet Draft,draft-guerrero-manet-saodv-03, 2005,

[4] F.-H. Tseng, L.-D. Chou, and H.-c. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," Human-centric Comput. In! SCi., vol. I, no. I, p. 4, 2011.

[5] Hoang Lan Nguyen , Uyen Trang Nguyen "A Study of different types of attacks in mobile adhoc networks ", Department of Computer Science and Engineering, pp. 2-7, 2012 .

[6] A. M. Kanthe, D. Simunic, and R. Prasad, "Eflects of malicious attacks in mobile ad- hoc networks," 2012 IEEE Int. Conf. Comput. Intell. Comput. Res., pp. 1-5, Dec. 2012 accessed on 20 Jan 2013

[7] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad HocinMANET”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3,September 2011, PP:Network,” IEEE Com

[8] Jagdish J. Rathod , Amit Lathigara,” Novel Approach of Preventing and Detecting Gray Hole Attack on AODV based MANET”, Volume 3, Issue 1, January 2015

[9] Sandeep Kumar, Mrs. Sangeeta Pramod Kumar Soni,” A Review on Gray Hole Attack in MANETs”, Volume 4, Issue 9, September 2014

DOI: 10.18535/ijecs/v4i8.17

[10] “An Efficient Wormhole Prevention in MANET Through Digital Signature” Anil Kumar Fatehpuria1, Sandeep Raghuwanshi, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 3, March 2013)

[11] A.Vani, D.Sreenivasa Rao, ”Removal of Black Hole Attack in Ad Hoc Networks to provide confidentiality Security Service”, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 3, March 2011.

[12]Pooja , Vinod kumar ,” A Review on Detection of Blackhole Attack Techniques in MANET’’International Journal of Advanced Research in Computer Science and Software Engineering, vol.4, issue 4, pp.364-368, 2014

[13]Neeraj saini , lalit Garg ,” Enhanced AODV Routing Protocol against Black hole Attack’’,International Journal of Advanced Research in Computer Science and Software Engineering, vol.4, issue 6, pp.847-850, June 2014

[14]Kriti Chadha , Dr. Sushmita Jain ,’’Impact Of Black Hole And Gray Hole Attack In AODV Protocol “,IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India

[15]. Asha Guddadavar , Bagali Ashvini A ‘’ Black Hole detection and avoidance in mobile Adhoc Networks’’, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 5 May 2015, Page No. 11854-11858.

[16] Gurnam Singh, Gursewak Singh ‘’ Detection and Prevention Of Black Hole Using Clustering In MANET Using Ns2’’ International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume - 3 Issue -8 August, 2014 Page No. 7420-7430.