INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
(Volume2, Issue5)
Available online at: www.ijariit.com

DETECTION OF GRAY HOLE ATTACK IN MANET

Geetanjali*
Electronics and Communication & HPTU
Gitanjalichauhan47@gmail.com

Anupama Kumari
Faculty of Electronics and communication & HPTU
er.anupma@gmail.com

Abstract-Mobile ad-hoc network (MANET) is a wireless network which has robust infrastructure. Mobile nodes can be used to form MANET. Arbitrary topology can be formed by connecting nodes with each other randomly. When source want to transfer packets to destination, a path being discovered for transmission. Sometime packets get dropped in path due to malicious node. Attack by malicious node is called gray hole attack. In this paper we detect the gray hole attack in the MANET. The detection and removal of the malicious node depends on the calculated probability of each node.

Keywords— malicious node, gray hole attack, MANET, probability, Arbitrary topology.

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a group of mobile nodes that cooperate and forward packets for each other. Such networks extend the limited wireless transmission range of each node by multi-hop packet forwarding, and thus they are ideally suited for scenarios in which pre-deployed infrastructure support is not available.[1] The applications of MANET include in business meetings, battlefield, hurricane , earthquake and other applications like personal area networking, sensor networks, mesh networks etc. In mobile ad-hoc networks because of dynamic routing frequent topology changes. In MANET routing involves three types of approaches, they are proactive approach, reactive approach, hybrid approach. AODV protocol is one of the on demand routing protocol and widely used in MANET routing.[2] A network can be wired network and wireless network. Wired network is that which used wires for communicate with each other's and wireless network is that which communicate without the use of wires through a medium .[6] Security is an essential factor in wireless ad-hoc network to have safety in transmitting data packets between two wireless sensor nodes.[5] . In a MANET, mobile nodes have the capability to accept and route traffic from their intermediate nodes towards the destination, i.e., mobile nodes can act as both routers and hosts. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes [7]. Security is an essential service for wireless network communications. Wireless mobile ad hoc nature of MANET brings new security challenges to network design. [3] Ad-hoc stands for temporary or for special purpose network. Here, each device is capable to maneuver or relocate severally in any direction or to any location. Each device must forward traffic that is not related to its own use, and therefore be a router.[10]

II. FEATURES OF MANET

MANET is advantageous with its several significant features of which some of them are listed below:
Autonomous Terminal: In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. Besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

***Distributed Operation*:** One of the features of MANET is nothing but distribution operation since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate among themselves and each node acts as a relay as needed, to implement functions security and routing etc.

***Multihop Routing*:** The IEEE 802.11 technology is a good platform to implement single-hop ad-hoc networks. Single-hop is that stations must be within the same transmission area (100-200 meters) to communicate. This limitation can be overcome by multi-hop ad-hoc networking which forwards packets via one or more intermediate nodes [3]. Related work is discuss in II section , a gray hole attack on MANET is discuss in III section , IV detection of gray hole and final conclusion is discuss in V section.

III. REVIEW OF LITERATURE

Jaydip Sen et. al[1], One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes may be compromised in such a way
that it may not be possible to detect their malicious behaviour easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. The proposed security mechanism increases the reliability of detection by proactively invoking a collaborative and distributed algorithm involving the neighbour nodes of a malicious gray hole node. Detection decision works on a consensus algorithm based on threshold cryptography. The simulation results show that the mechanism is effective and efficient with high detection rate and very low false positive rate and control overhead.

Usha G^1 et. al[2], AODV protocol is a routing protocol which are type of demand-driven protocols. Before understanding the vulnerable behavior of the protocol, understanding the working of the protocol is important AODV is known as on-demand because it invokes only when a node has data to transmit. It uses IP addressing
and uses UDP as the transport layer protocol which offers either error recovery or flow control.

Onkar V.Chandure et. al[3], Performance is the main term for any network but because of some attacks such as gray hole attack as main in the network performance gets degrade. In this paper we have implemented the AODV protocol with PDR & e2e term & also analyze the impact of gray hole attack on ad-hoc network, with their PDR & e2e value. Simulation of AODV as well as gray hole attack is carried out by using ns-2 tool & performance of AODV implementation is carried out before the gray hole attack on ad-hoc network as well as after the gray hole attack on AODV protocol. To show the effectiveness and results of proposed approach, implementation work on Network Simulator 2 tool is still in progress phase. Future works will includes some method to secure the ad-hoc network from the gray hole attack & also improve the performance of the network & make the network well efficient.

Parineet D.Shukla et. al[4],a analytic approach towards detection and removal of gray hole attack in the network. The probability of each node is calculated and depending on that the node can be detected as malicious and removed from the network. The solution depends on the behavior of the node in the particular network. For securing the network it is important that each node in the network must be honest i.e. it must forward all the incoming packets to the next node in the path. When a node drops some packets the data which is to be transmitted does not reach to the destination correctly. Detection of gray hole attack is important to ensure proper transmission of data.

IV. GRAY HOLE ATTACK ON MANET

Gray Hole attack is the attack on the ad-hoc network .Gray Hole attack can be act as a slow poison in the network side means we can't said that probability of losing the data. In Gray Hole Attack a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective. Every node maintain a routing table that stores the next hop node information for a route a packet to destination node ,When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in its routing table. Otherwise, nodes initiates a route discovery process by broadcasting *Route Request* (RREQ) message to it's neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A *Route Reply* (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination. We now describe the gray hole attack on MANET'S .The gray hole attack has two important stages , In first stage, a malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intension of interrupting or corrupting packets, event though route is spurious. In second stage, nodes drop the interrupted packets with a creation probability. Detection of gray hole is difficult process. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack. A variation of black hole attack s is the gray hole attack, in which nodes either drop packets selectively

(e.g. dropping all UDP packets while forwarding TCP packets) or drop packets in a statistical manner (e.g. dropping 50% of the packets or dropping them with a probabilistic distribution). Both types of gray hole attacks seek to disrupt the network without being detected by the security measures in place [3].

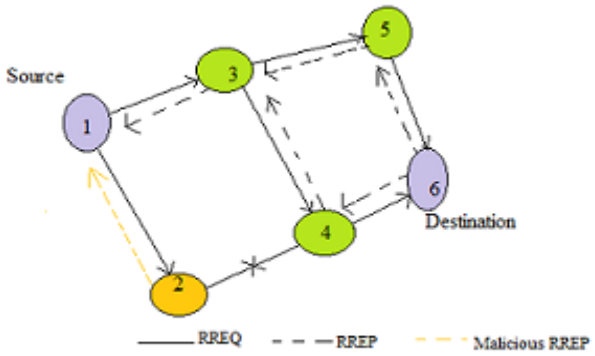

Fig 1. Gray hole attack in MANET

V. DETECTION OF GRAY HOLE ATTACK

In recent work the gray hole attack is detected depending upon the count of the false reply getting from the next node [4].

1. The gray hole detection procedure

In the detection of gray hole attack three stages are process.
a). Firstly checked the path of network whether there is malicious node is present or not.
b). Secondly checked the node behavior and if node is malicious then that node can be removed from the path.
c). In last process when malicious node is removed then a new path make and all the packets are transfer from that path.

i) Discovery of route in network

When a transmitter node transmit the packet to destination node its first work is to find its route cache, it checked the previous discovered route. If there is no route found in its route cache, the transmitter node find the new route to the destination node by route discovery process. Each request message has source and destination unique identification and intermediate nodes addresses list. When request message is reached at the destination node, then destination node gives a feedback message to transmitter node to have inside the track for the route request message. When feedback message received at the transmitter node, in order not to repeat the discovery process for each new packets that are destined to the target node its caches the path in its route cache. While receiving a route request message, a node which has seen another route request message with a same request identification and destination address from the same transmitter, then that particular node discards the received request message. The node discards the received request message if it is already enlisted in the route path of the route request message. Otherwise the node connects its address to route path record of the route request message and broadcast it with the same request identification.
The fig.2 shows the discovery of route in network. If node transmit a packet, node N6 do not have any direct route to their cache. Node N1 broadcast request packet and N2 and N3 receive it. The request packet is connected with their addresses and the message is broadcasted again. When node N2 and N3 is processing the request, the retransmitted request will be discarded, now node and request is received by node N4 and its address is added and then again it broadcasted.

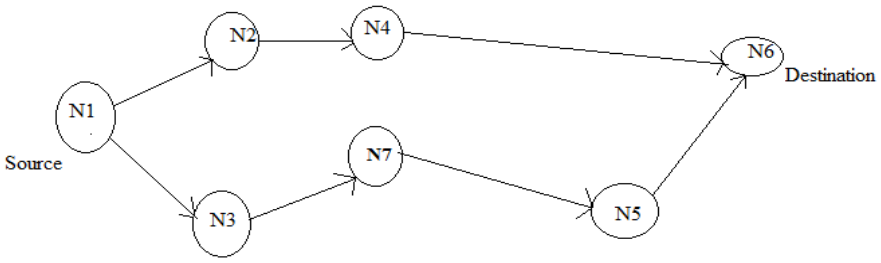

Fig.2 Route Discovery

The request from the node N3 is receive and broadcasted by node N7. Finally, any future reception is discarded, when request is received by node N6 form node N7. The route through which, the connection is establish between node N1 and node N6 is N1-N2-N4-N6.

2. Packet forwarding probability

The information that has been send to destination by the transmitter is forwarded in form of the packets. All the packets are combined at the receiver end of the network to get the information which is transmitted by the transmitter. For participating in route the all packets are travel through each node. If that time a malicious node is present in the path then it gives a fake reply to the packet forwarded, so this is prior to detect the probability of fake reply from the specific node.

The forwarding of the packet to the next node and reply to the request is done at the same time. A fake reply is generated and stored in previous node, if the packet is not forwarded from the node. If the node is either malicious or can't be checked then it has a greater probability of getting a fake reply from a specific node. The probability of getting a fake reply from specific node is

P(FR)= Total no. of fake reply/Total no. request sent

R. NO.	AUTHOR NAME	YEAR	TECHNOLOGY USED	DESCRIPTION
1.	Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar	2007	NS2	A security mechanism is proposed to defend against a cooperative gray hole attack on the well known AODV routing protocol in MANETs.
2.	Usha G1, Bose S2,	2013	NS2	Gray Hole attack model is developed for AODV protocol. Experiments are simulated for Gray Hole attacks under variety of ad-hoc network condition.
3.	Onkar V.Chandure, V.T.Gaikwad	2012	NS2	Describe the basic idea related with the implementation of AODV protocol & impact of gray hole attack on ad-hoc network.
4.	Parineet D. Shukla, Ashok M Kanthe , Dina Simunic	2014	NS2	The probability of the each is calculated and depending on that that node can be detected as malicious and removed from the network.
5.	Praveen K S,Gururaj H L,Ramesh B	2016	NS2	Detect black hole attack from the ad-hoc by using AODV and OLSR protocols
6.	Bo Sun,Young Guan,Jian Chen, Udo W.Pooch	2003	NS2	A general approach for detecting black-hole attacks in mobile ad hoc networks, which due to their

				mobility and being broadcast in nature, are particularly vulnerable to attacks compared to traditional wired networks.
7.	Gao Xiapoeng,Chen Wei	2007	NS2	Most of the malicious nodes could be detected, the routing packet overhead was low, and the packet delivery rate has been improved with the help of three purposed algorithm. : the creating proof algorithm, the checkup algorithm and the diagnosis algorithm.
8.	Avenash Kumar 1, Meenu Chawla 2	2012	NS2	Detection of group gray hole attack through destination based scheme when more than one malicious nodes are in a Mobile ad hoc network.
9.	Supriya Pustake1, Dr. S. J. Wagh2, D. C. Mehetre3	2016	NS2	Detection of gray hole attack by pool tile method
10.	Kusumlata Sachan, Manisha Lokhande	2016	NS2	Security threats and AODV routing protocols along with gray-hole attack to investigate the need of preventive mechanism for better performance.

CONCLUSION

In this paper we detect the gray hole attack by checking of fake reply in the network, in this paper work we check the route of the network in which data is transmit from source to destination. It check the probability of the malicious node which are present in network, by probability check we can detect the malicious node. With future emphasis given for the secure transmission, we can prevent the MANET by malicious node using different methodology

REFERENCES

[1]Sen, J., Chandra, M. G., Harihara, S. G., Reddy, H., & Balamuralidhar, P. (2007, December). A mechanism for detection of gray hole attack in mobile Ad Hoc networks. In *Information, Communications & Signal Processing, 2007 6th International Conference on* (pp. 1-5). IEEE.

[2]Usha, G., & Bose, S. (2013, February). Impact of Gray hole attack on adhoc networks. In *Information Communication and Embedded Systems (ICICES), 2013 International Conference on* (pp. 404-409). IEEE.

[3]Chandure, O. V., & Gaikwad, V. T. (2012). Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol.*International journal of computer Applications*, *41*(5).

[4]Shukla, P. D., Kanthe, A. M., & Simunic, D. (2014, December). An analytical approach for detection of gray hole attack in mobile ad-hoc network (MANET). In *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on* (pp. 1-5). IEEE.

[5]Praveen, K. S., Gururaj, H. L., & Ramesh, B. (2016). Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols.*Procedia Computer Science*, *85*, 325-330.

[6] Sun, B., Guan, Y., Chen, J., & Pooch, U. W. (2003, April). Detecting black-hole attack in mobile ad hoc networks. In *Personal Mobile European (Conf. Publ. No. 492)* (pp. 490-495). IET.

[7] Xiaopeng, G., & Wei, C. (2007, September). A novel gray hole attack detection scheme for mobile ad-hoc networks. In *Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on* (pp. 209-214). IEEE.

[8]Kumar, A., & Chawla, M. (2012). Destination based group Gray hole attack detection in MANET through AODV. *IJCSI, ISSN (Online)*, 1694-0814.

[9]Pustake, S., Wagh, S. J., & Mehetre, D. C. Gray Hole Detection and Removal in MANET by Pool Tile Method.
[10]Sachan, K., & Lokhande, M. (2016). An Analysis of Gray-hole Attacks on Mobile Ad-hoc Networks. *International Journal of Computer Applications*,*146*(14).

