ISSN:0975-9646

Gray-hole Attack in Mobile Ad-hoc Networks : A Survey

Rupali Sharma

Student, M. Tech (Computer Science),
Department of Computer Science, Sanghvi Innovative Academy
Indore.

***Abstract*— Mobile ad-hoc network (MANET) is a wireless network that can transfer the information from source to destination wirelessly. Now days this network is widely used all around the world because it does not require any fixed wired network to establish communication between the source and the destination. The entire network can be established by using transmitter, receiver, processor and the battery. In today's scenario the mobile ad hoc network used in many real time applications like military surveillance, disaster management, air pollution monitoring etc.**

Due to the open communication media the mobile ad-hoc network has some security limitations there are the possibility of information leakage in the network. Many researchers are working on it to achieve the privacy concern. Gray-hole attack, black-hole attack, wormhole attack are the major threats in the mobile ad-hoc network. In gray-hole attack selective dropping of the packets occurs, and the information cannot be further transmitted .this research paper investigate the appropriate solutions and developed the suitable solution to prevent the network from the gray-hole attack.

***Key words*— MANET, AODV, Black-hole-attack, Gray-hole Attack**

I. INTRODUCTION

Mobile ad-hoc Networks refers to a group of spatially dispersed and dedicated nodes for monitoring and recording the physical conditions of the environment and helps to measure environmental conditions like temperature, sound, Pollution levels, humidity, wind speed and direction, pressure etc. MANATEs also used in organizing the collected data at a central location. In the traditional networks wired communication link with depended infrastructures are used to create connections among nodes. Here, they required base stations or routers to interconnect nodes. For example, mobile phones need to connect with base stations; PDAs or laptops have to connect with access points or RJ-45 cable. Wired connection and infra is the backbone of such network and they lose the connection when leave the access point. Mobile ad-hoc network is the collection of mobile node deployed with temporary purpose. Mobile ad-hoc network can be infrastructure-less or based on fixed infrastructure. It allows mobile node to communicate with each other independently Here, every node is self-configurable node and capable to transmit, receive or forward packet as per requirement. Every node can work as router and help to discover route among nodes.

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 behavior easily. Malicious nodes can generate new routing messages to advertise nonexistent links and provide incorrect link state information, and flood other nodes with routing traffic. One of the widely known attacks is the Gray Hole Attack. It is the variation of Black hole attack. Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network and that node drops the entire packet. But in Gray-Hole attack, nodes will drop the packets selectively.

Furthermore, black-hole is the subsequent threat of wormhole attack on network and transport layer, where malicious node misguides the source node by using shortest path attraction. The complete study concludes that Wormhole attack, Black-hole attack and Gray-hole attack lies in same category but having different damage mechanism. Gray-hole attack is launched by single malicious node or cooperatively by a set of malicious nodes.

Among the various protocols available AODV is most vulnerable to such attack. In AODV every mobile node maintains a routing table that stores the next hop node information for a route to a destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if such a route is available in its routing table. Otherwise, the node initiates a route discovery process by broadcasting a Route Request (RREQ) message to its neighbors. On receiving a RREQ message, the intermediate nodes update their routing tables for a reverse route to the source node. All the receiving nodes that do not have a route to the destination node broadcast the RREQ packet to their neighbors. Intermediate nodes increment the hop count before forwarding the RREQ. A RouteReply (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 the destination.

II. LITERATURE REVIEW

A lot of researches in the last some years are estimated and implemented but the most significant contributions were the trust based security. In a challenge to improve security in MANET lots of researchers worked in a field, some have suggested new techniques and implemented innovative improvements in the protocols and some of them have recommended new protocols. There are various types of attacks which try to degrade the performance of the network. Flooding attacks occur when a network becomes so heavily traffic loaded with unnecessary packets initiating requests for link that it can no longer process authentic connection requests. Flooding is reason for traffic and congestion in the network and thus incompleteness of legal connection. Once this buffer is full with request packet traffic become uncontrolled no extra connections can be made, and the result is a Denial of Service Jaydeep Sen at. el. [10] proposed a mechanism to detect gray-hole attack by selecting alternate path towards the ultimate destination. They also proposed a technique to prevent ad-hoc network from this hazardous attack using alarm message and bypass malicious node. Due to irregular behavior of gray-hole attack, it is complex task to detect and prevent during communication. Proposed method increase the security mechanism and reliability factor of detecting malicious node by proactively involving the neighbor nodes of a malicious gray-hole attack.

Sukla Banerjee [9] proposed a mechanism for detection/removal of cooperative black and gray-hole attack in mobile ad-hoc networks. In this instead of sending the total data traffic at a time it divide the total traffic into some small sized blocks. So that malicious nodes can be detected and removed in between the transmission of two such blocks by ensuring an end-to-end checking. Source node sends a prelude message to the destination node before start of the sending any block to alert it about the incoming data block. It is time consuming algorithm it takes time in converting of total traffic into small sized blocks.

Mechanism for detection of gray hole attack in mobile ad hoc network are proposed by Jaydip sen, M. Girish Chandra, Harihara S.G.[10]. They proposed a mechanism to detect and defend the network against such an attack which may be launched cooperatively by a set of malicious nodes. The proposed security mechanism increases the reliability of detection by proactively invoking a collaborative and distributed algorithm involving the neighbor nodes of a malicious gray-hole node. Detection decision works on an algorithm based on threshold cryptography. Simulation results show that the mechanism is effective and efficient with high detection rate and very low false positive rate and control overhead.

Ahmed, M. et. al.[1] address that gray-hole is the successor of blackhole attack which not only drop the respective packets but also create illusion between trusted node and attacker identity. They have used ids technique with voting attribute to identify attacker node and create difference between trusted node and attacker node. The proposed system is simulated using NS-2.35 simulator and configured into Debian Linux 6. They have used AODV routing protocol for route discovery and modify the proposed solution named for black-hole and gray-hole attack.

III. GRAY-HOLE ATTACK

A gray-hole attack is extension of black-hole attack used to bluff the source and monitoring system by partial forwarding. Here, attackers uses selective data packet dropping method to behave as genuine node and try to participate into full communication. Gray-hole malicious node participate into route discovery process and update the source route cache/ routing table as shortest path. Afterwards, source always consider malicious node as next hop node and forward packet to same. Malicious node captures all the incoming packets but drop on random basis. The complete phenomena create toughness against detection and prevention mechanism because harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, congestion or selfish nature. Gray-hole attack may apply through two ways which are listed below;

1. Dropping all incoming UDP packets.
2. Partial dropping of UDP packets with random selection process.
3.

Gray-hole is an attack that can switch from behaving genuine to sinkhole. Because it can act as normal node switch over to malicious node it becomes too typical to identify the state whether it us normal node or malicious node.

In the ad-hoc on demand distance vector (AODV) routing process every node carry a routing table having ultimate destination and next hop information. This information is used to discover route from source to destination. Here, every node check routing table to know whether the route is available or not. In case of indirect communication it forward packets to next hop node to forward packet to destination.

The gay-hole attack has two phases which are listed below;

A. *Phase1*

In this phase malicious node exploits the vulnerabilities of AODV routing protocol and update the source routing table as shortest route in next hop column. The main objective of this update is to divert all the packets to malicious node rather than genuine route.

B. *Phase 2*

It is the implementation phase of gray-hole attack where malicious node dropped the interrupted packets with a certain probability. A probabilistic method is use for packet selection. In the normal situation, attacker node changes the behaviors rapidly. Thus, sometime it transfer packet and some time it drop the packets. Furthermore, in the state of malicious node it also forwards some packet to create illusion of genuine nodes. Due to this behavior it is very hard to find out in the network to figure out such kind of attack.

Figure 1 shows the block representation of selective dropping

C.

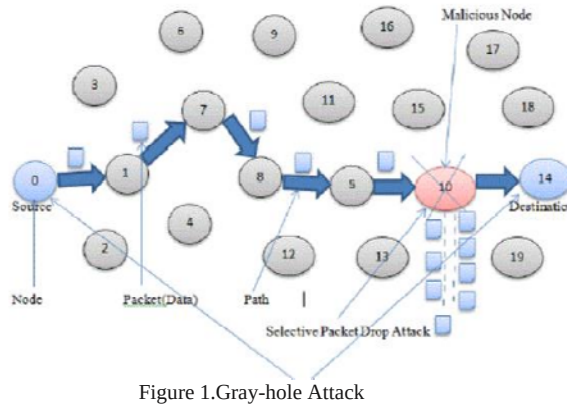


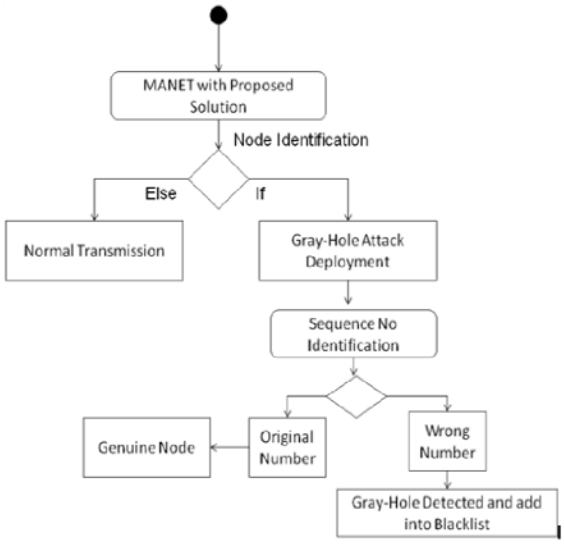
Figure 1.Gray-hole Attack

IV. PROBLEM INVESTIGATION

The AODV routing protocol is a popular reactive routing protocol in wireless networks, but AODV routing protocol designed for better performance of the network not for security of node, secure protocols are generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. For security purpose it have vulnerabilities and it is easily manipulate by malicious node to destroy its network routing. The open nature of wireless medium also makes it easy for outsider attackers to interfere and interrupt the legitimate traffic. This concept classifies the attacks into two broad categories, namely Passive and Active attacks. In Passive attack, the adversary only eavesdrop upon the packets content, while packets may get dropped or altered on way in case of Active attacks. One of the widely known attacks is the Gray Hole Attack. It is the variation of Black hole attack. Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network and that node drops the entire packet. But in Gray-Hole attack, nodes will drop the packets selectively. The complete study observes that, AODV is a insecure routing protocol and does not incorporate any mechanism to detect and prevent communication from malicious affect.

IV. SOLUTION DOMAIN

The need and problem definition specifies that, proposed strategy should detect network vulnerabilities in the MANET. The study will be based on detection of Gray-Hole attack and prevent the network from same. Here, complete study observes that, there are several techniques proposed to detect and prevent gray-hole attack using multipath solution. Ahmed, M. et. al.[1] proposed a side technique with voting attribute to identify attacker node and create difference between trusted node and attacker node.. A dynamically strong technique has been proposed in this section which describes the complete methodology to detect and prevent malicious node. The basic idea behind the proposed technique is based on Intrusion Detection System. In the proposed solution every mobile node carries intrusion detection system which monitors the complete network structure with in-built mechanism. IDS estimate the count value of sequence number to measure the suspicious factor according to RREQ and RREP packet counting. When a suspicious value for a neighboring node exceeds a threshold, then that node is isolated from the network as other nodes do not forward packets through the suspected malicious node.



Fi

gure 2: Proposed Architecture

V. CONCLUSION

The complete study concludes that AODV and modified-AODV are most popular and useful routing protocol for establishment of MANETs. It also observed that, they do not have any security policy and vulnerable for various security threats. Hostile Environment may lead to harm it performance in unbelievable manner. There is need to identify the vulnerabilities and increase its growth. The complete work observes Gray-hole attack as crucial threat and will propose a solution to overcome its problem.

REFERENCES

[1] S. marti, T.Guili, K. Lai, & M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", In proceedings of MOBICOM 2000.

[2] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-organized network-layer security in mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, February 2006.

[3] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03).

[4] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference on Ubiquitous information management and communication, 2008.

[5] A. Nadeem, M.Howarth " Protection of MANETs from a range of attacks using an intrusion detection & prevention system" published in Springer science + Business Media in 2011.

[6] H. Deng, H. Li, and D.P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, October 2002.

[7] M. Jackobsson, J. Hubaux, and L. Buttyan, "A micro-payment scheme encouraging collaboration in multi-hop cellular networks," In Proceedings of Financial Crypto 2003.

[8] Padilla, E., Aschenbruck, N., Martini, P., Jahnke, M., & Tolle, J. (2007). Detecting black hole attack in tactical MANETs using topology graph. In Proceeding of 32nd IEEE conference on local computer networks.

[9] Sukla Banerjee "Detection/Removal of Cooperative Black & Gray Hole Attack in MANETs" in proceedings of the World Congress on Engineering & Computer Science 2008.
[10] Jaydip Sen, M.Girish Chandra, Harihara S.G. "A Mechanism For Detection Of Gray Hole Attack in Mobile Ad Hoc Networks" published in IEEE Journal in 2007.
[11] V. SHANMUGANATHAN, Mr.T.ANAND M.E.," A Survey on Gray Hole Attack in MANET" IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 22503501 Vol.2, No6, December 2012.
[12] Parineet D. Shukla, Ashok M. Kanthe, Dina Simunic "An Analytical Approach for Detection of Gray Hole Attack in Mobile Ad-hoc Network (MANET)" published in IEEE 2014.
[13] Ashok M.Kanthe, Dina Simunic and Ramjee Prasad "Effects of Malicious Attacks in Mobile Ad–hoc Networks" published in IEEE Journal in 2012.
[14] Mozmin Ahmed and Md. Anwar Hussain "Performance of an IDS in an Adhoc Network under Black Hole and Gray Hole attacks" published in IEEE in 2014.
[15] G.Usha and Dr.S.Bose "Impact of Gray Hole Attack on Adhoc networks" published in IEEE Journal 2014.