International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-3, March 2016
ISSN: 2395-3470
www.ijseas.com

An Approach To Mitigate Gray-hole Attack In Mobile Ad-hoc Networks

Neha Patidar, Pritesh Jain

Patel College of Science and Technology, Indore, India

Patel College of Science and Technology, Indore, India

Abstract

Mobile ad-hoc networks are collection of electronic mobile devices which can be easily relocates and moves from one place to another place. Mobile nodes are integrated collection of transmitter, receiver, battery and processor for establishment of networks. It uses wireless communication media for communication and transfer information from one place to another. Mobile nodes and its networks have several characteristics can be deployed into various situations like military surveillance, disaster management, rural and jungle areas etc. Furthermore, it has certain weakness which can be power constraint, security threats, routing overhead, QoS, network breakdown, environmental impact etc. Open nature of communication media make it vulnerable for various security threats and may degrade its performance as well.

Security is the major limitation of wireless natured network, can be exploiting for leakage of information. Thus, privacy achievement is measure concern and most research area for same. Several security threats like wormhole attack, blackhole attack, Gray-hole attack, Sybil attack, jamming may be used by attacker to compromise the network security. Gray-hole attack is one of severe security threat which not only compromises the network but also partially drop forwarded packets. This research paper investigates certain solutions and developed most suitable solution to mitigate gray-hole attack in MANET. NS-2 simulator has been used to simulate and evaluate the performance of proposed solution

Keywords: MANET, AODV, Gray-hole Attack, NS-2 Simulator

1. Introduction

A Mobile ad-hoc network is self-configurable wireless networks uses infrastructure-less technology for mobile node deployment and connections. Ad-hoc stands for temporary network which is deployed for a particular purpose. Here, each device is capable to work as switch, bridge and router to transmit and forward packets respectively.

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. Wireless technology is allowing to access information and services electronically from everywhere. Wireless technology has become tremendously popular due to its usage in various new fields of applications in the domain of networking. Protecting the network layer from malicious attacks is an important and challenging security issue in mobile ad hoc networks (MANETs).

Mobile Ad hoc Network (MANET) are used most commonly all around the world, because it has the ability to communicate each other without any fixed network. Security is an essential requirement in MANET. Without any proper security solution, the malicious node in the network will act as a normal node which causes eaves dropping and selective forwarding attack generally known as gray-hole attack**.**

MANETs are vulnerable to various types of attacks including passive eavesdropping, active interfering, impersonation, and denial-of-service attack. 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 behavior 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. 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. Because gray-hole attack lies in same category of wormhole attack, it can be deployed with any technique of wormhole attack.

Among the various protocols available DSR is most vulnerable to such attack. In DSR 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 RouteRequest (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.

The study observe that security policy development is the most vital area for researchers and illegal access of resources or services is dangerous as like leakage of data or information. This illegal interception may be reason for network breakdown or failure of communication. In this manner, routing protocols are also responsible and give impact on performance of networks. Routing protocols are used for route searching and information delivering from source to destination. A major portion of research work is also dedicated to enhance the performance of routing protocol and performance.

2. Literature Review

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.

3. Gray-hole Attack

A gray hole attack is a variation of black hole attack, where an adversary first behave as an honest node during the route discovery process, and then silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. Detection of gray-hole attack is 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 is also known as selective forward attack. Selective forward attack is of two types which are:

1. Dropping all UDP packets while forwarding TCP packets.
2. 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.

Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node. If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbor, by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source. A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination.
The gray-hole attack has two phases:

Phase 1:

A malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intention of interrupting packets of spurious route.

Phase 2:

In this phase, the nodes has been dropped the interrupted packets with a certain probability and the detection of gray-hole attack is a difficult process. Normally in the gray-hole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Both normal node and attacker are same. Due to this behavior it is very hard to find out in the network to figure out such kind of attack.

4. 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.

5. 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. Jaydeep Sen [10] proposed a technique based on alarm and alternate neighbor route mechanism. This is capable of detecting & preventing the single & cooperative malicious gray-hole nodes. Once a node is detected to be really malicious, the scheme has a notification mechanism[Alarm Message] for sending messages to all the nodes that are not yet suspected to be malicious, so that the malicious node can be isolated and not allowed to use any network resources. The mechanism consists of four security procedures which are invoked sequentially. The security procedures are:

(1) Neighborhood data collection,

(2) Local anomaly detection

(3) Cooperative anomaly detection

(4) Global alarm raiser.

Malicious node is isolated from the network by generating an alarm messages which can cause an extra overhead in the network. They provide a solution which can overcome the overhead of network caused by source node

who send alarm message to all the other node about the gray-hole node. The complete work concludes that, proposed solution will be based on above explained technique and try to improve network performance.

6. 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.

Reference

[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.