MITIGATION OF GRAY-HOLE ATTACK IN MOBILE AD-HOC NETWORKS

Neha Patidar,Patel College of Science and Technology, Indore, India

Pritesh Jain, Patel College of Science and Technology, Indore, India

ABSTRACT

Mobile ad-hoc network is collection of self configurable mobile nodes with infrastructure-less topology connected without wires. Ad-hoc stands for temporary or for special purpose network. Here, every device is capable to move or relocate independently in any direction or to any location. Each must forward traffic unrelated to its own use, and therefore be a router.

The major challenge to construct such network is to maintain the connection without any interrupt. Here, every node can forward packet to next hop and manage route traffic. Such network may work independently or may connect to large network such as internet. The result make it dynamic and very scalable, flexible solution for connect each other. Open nature of communication makes it vulnerable for various security threats and malicious attack may try to compromise the communication. Thus security is the major security challenge.

This research paper considers Gray-hole as the malicious attack and tries to explore the prevention technique for same. This work tries to propose a novel technique to detect malicious node and develop a technique to prevent network from same. The complete work is implemented with NS-2.35 environment and evaluated on basis of mobile and stationary state on various scenarios.

1. INTRODUCTION

Mobile ad-hoc network is the collection of mobile node deployed with temporary purpose. It may be infrastructure-less or based of fixed infrastructure. It allows to mobile node to communicate with each other without using third party devices. 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.

Mobile ad-hoc network advancement provides many reimbursements which are;

- Ad-hoc networks are easy to set up and cheap to deploy
- Mobility and relocation gives freedom to access and shifting
- Flexible and Scalable
- Low cost network solution

MANETs are vulnerable for various security threats which may include active or passive approach. It may include eavesdropping, interfering, DDOS, wormhole, Gray-hole attack etc. All such attacks not only attempt to compromise the privacy of communication but also degrade the performance by dropping the packets. The most critical problem with such network is vulnerability in routing protocols. Most of the routing protocols are designed as per resource

ISSN: 2278 – 1323

constraint and better performance during wireless situation. None of them is designed with security policy and keep data or node safe from other malicious nodes.

In this manner, Gray-hole attack is one of the severe security threats which not only compromise the security of network but also degrade the performance by dropping the packets.

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.

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 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.

Routing Protocols:

Routing protocols are set of rules which are used to discover routes among nodes. These are classified into three categories which can be listed below;

1. Proactive Protocols
2. Reactive Protocols
3. Hybrid Protocols

Proactive routing protocols are set of rules that discover on prior basis before getting the request. They are also known as table driven protocols monitor the network topology continuously to observe the route for all possible destination. Every node maintain routing table to store routes and relevant information. Routes are updates for all possible nodes periodically during throughout execution.

Reactive routing protocols are on demand routing protocols used to discover routes based on request. They discover routes as the reaction of route discovery request and invoke route determination practice on require only. AODV, DSR are the most popular routing protocols of this schemes.

This paper considers AODV as the routing protocol for information communication. AODV is a reactive routing protocol intended for ad hoc

ISSN: 2278 – 1323

networks. Ad-hoc networks are temporary kind of network deploy for special purpose. Here, AODV is on-demand protocol specially designed for temporary network and can be suited for dynamic self-configured networks such as ad-hoc network. AODV provides loop free paradigm with strategic route management for broken links. It has very low bandwidth requirement and AODV has low overhead comparatively less than other protocols as AODV does not require periodic route advertisements. It implies three kind of routing protocols which can be listed below;

1. Route Discovery through RREQ [Route Request] Message
2. Route Response through RREP [Route Reply] Message
3. Error Recovery through RERR [Route Error Recovery] Message

Security of Network Operations:

Due to open nature of communication, there are many reasons which push the ad-hoc network into danger condition. When unapproved node or entities disrupt the normal operation, we can say the network is under assault. When different nodes communicating with each other by a wireless medium and all this are vulnerable to connect attacks some of the links attack are:

- Submissive eavesdrop
- Dynamic snooping
- Leaking clandestine information
- Data changing
- Masquerade
- Message respond
- Message deformation
- DOS

The majority of the security necessities require not be tended to in the system or upper layers. For example, in a few remote LANs connection layer encryption is connected. Be that as it may, as a rule the security administrations are actualized in higher layers, for example, in the system layer, since numerous specially appointed systems apply IP-based steering and propose or recommend the utilization of IPSec.

The recognition of compromised node is one of the biggest problems. Frequently such nodes can be discovered by observing their behavior, but because of their unfortunate link quality sometimes other nodes misbehave as well. A complicated failure has mainly happened due to the presence of negotiating node.

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.

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.

ISSN: 2278 – 1323

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.

2.SOLUTION DOMAIN

The objective of this research work is to explore the most suitable solution to mitigate gray-hole attack and improve the performance of AODV as well as MANET during insecure situation. Gray-hole attack is the family member of Wormhole attack and Black-hole attack; those are used to drop packets at source node or intermediate node to degrade the performance. The issue with this two attack is 100% dropping. Complete dropping can be strong symptom to detect adversary and mitigate the malicious node. Gray-hole attack removes the weakness and start selective dropping. Technique for node deployment and malicious node compromise is remaining same.

A dynamically strong technique has been proposed in this section which describe 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 athreshold, then that node is isolated from the network as other nodes do not forward packets through the suspected malicious node.

3. RESULT OBSERVATIONS

The following metrics are used in this work for comparing the performance of AODV, AODV under attacks and Modified AODV routing protocols.

1. Throughput
2. Packet Delivery Ratio(PDR)
3. End-to-End Delay(E2E)

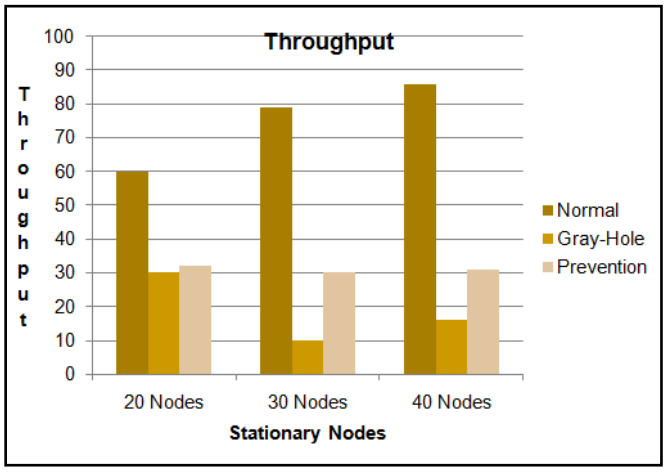

Figure 1.1: Throughput Analysis of Stationary Nodes

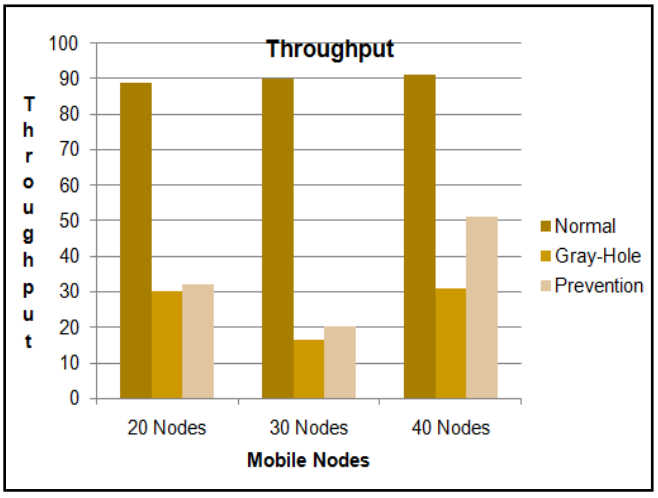

Figure 1.2: Throughput Analysis of Mobile Nodes

ISSN: 2278 – 1323

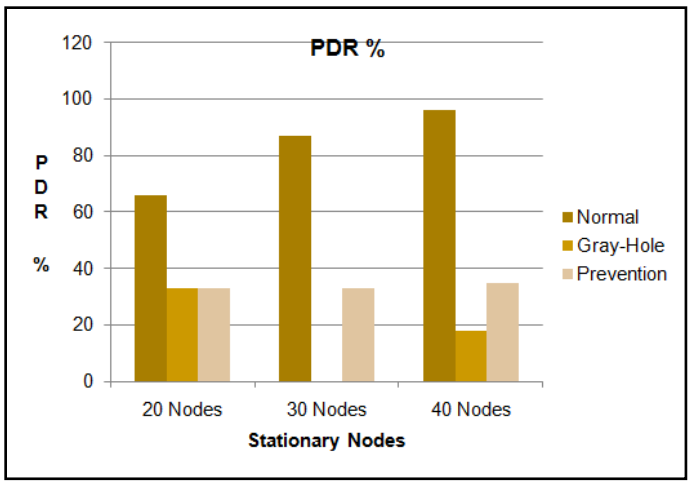

Figure 1.3: PDR Analysis

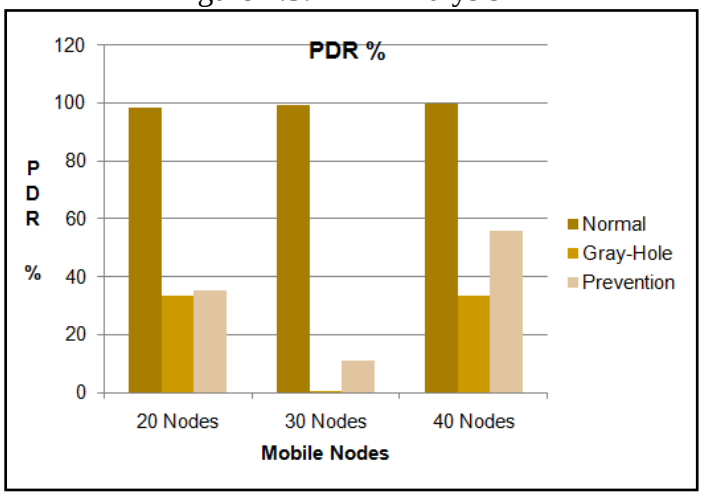

Figure 1.4: PDR Analysis

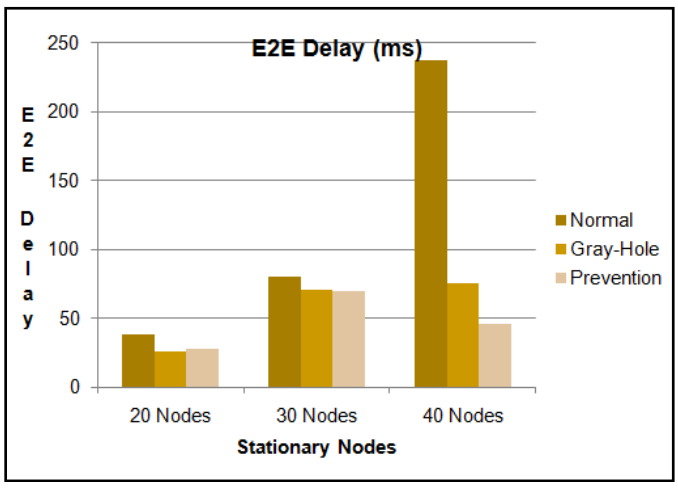

Figure 1.5: End-To-End Delay Analysis

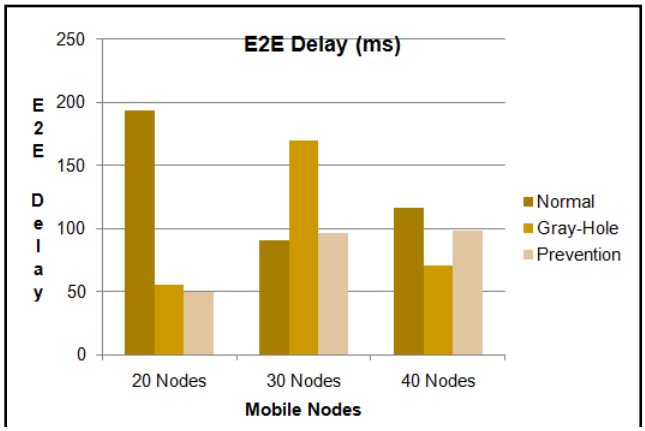

Figure 1.6: End-To-End Delay Analysis

4. CONCLUSION

This research work carried out a study and analysis of AODV routing protocol with various security threats. The complete work concludes that security threats not only harm the performance of ad-hoc network but also leak the privacy and confidentiality of content. It may lead to destruction of network. A Gray-hole attack is consider as the malicious attack to observe the impact of malicious node on network and prevention technique has been developed to mitigate the same.

The complete work concludes that Gray-hole attack is one of the severe security threat which not only partially drop packet but also compromise the communication. This phenomena lead to degrade the network performance and compromise the network security. A IDS based mechanism with highest sequence number technique has been used to detect and mitigate gray-hole attack in ad-hoc network.

REFERENCES

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

ISSN: 2278 – 1323

[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.

ISSN: 2278 – 1323