Mitigation of Gray-Hole Attack in MANET

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

ABSTRACT-Mobile ad-hoc networks are set of nodes deployed in mobile situation. It may deploy into two states either in static situation or in mobility state. Due to low weight and mobility feature they can easily relocate and move from one place to another location. A mobile node consist the certain basic elements which can be listed as battery, transmitter, receiver and process for establishment of networks. A wireless communication is used to send and receive information among nodes. Due to wireless communication media does not imply any infrastructure and gives a structure free topology. Mobile nodes and ad-hoc network have several features and can suitable for various applications like military surveillance, disaster management, rural and jungle areas etc. Subsequently, it also have certain loopholes can be listed as resource constraint, security issues, routing overhead and network breakdown.

Security is one of the major concern and also the limitation with ad-hoc network. It address that privacy is one of the important requirement into every communication. The work conclude that several security threats like wormhole attack, black-hole attack, gray-hole attack etc. are the severe security threats which not only disrupt the network but also degrade the network performance.

The complete work observes that gray-hole attack is one of the severe security threats which not only try to get beneficial of vulnerability in routing protocol but also drop packets respectively. This research paper investigates the impact of gray-hole attack and also derived a mechanism to overcome it.

NS-2 simulator has been used to simulate and evaluate the performance of proposed solution

Keywords: MANET, AODV, Gray-hole attack.

I. INTRODUCTION

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 wireless communication revolution is bringing fundamental changes to data networking, telecommunication, and is making networking and communications, anytime, anywhere possible.

A) Mobile ad-hoc network advancement provides many reimbursements which are;
B) Ad-hoc networks are easy to set up and cheap to deploy
C) Mobility and relocation gives freedom to access and shifting
D) Flexible and Scalable
E) Low cost network solution

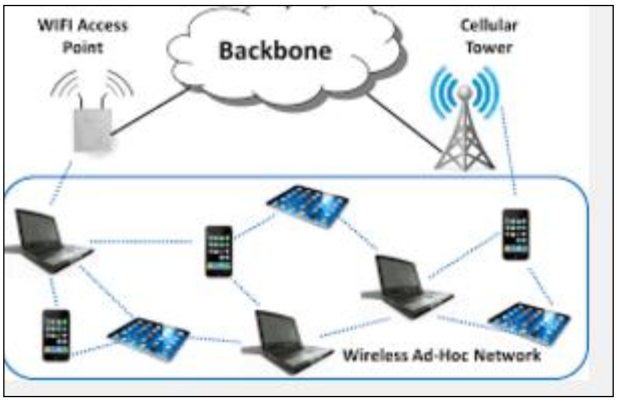


Figure 1: Block Diagram of MANET

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.

.

II. LITERATURE REVIEW

The study of complete work concludes that ad-hoc network is vulnerable for various security threats due to open wireless communication medium. It is susceptible for various security threats. Various researchers have done research in this field and consider black-hole and gray-hole attack as the severe security threat which can apply due to vulnerability in routing protocols. It can state as the routing disruption attack.

Ahmed, M. et. al.[1] address that gray-hole is the successor of black-hole 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.

The study of gray-hole attack conclude that Gray-hole malicious node participate into route discovery process and update the source route cache/ routing table as shortest path. Because AODV doesn't implies any security measures it can't detect malicious node. Subsequently, it is highly vulnerable for security threat approaches.

Gray-hole attack may apply through two ways which are listed below;

A) Dropping all incoming UDP packets.

B) Partial dropping of UDP packets with random selection process

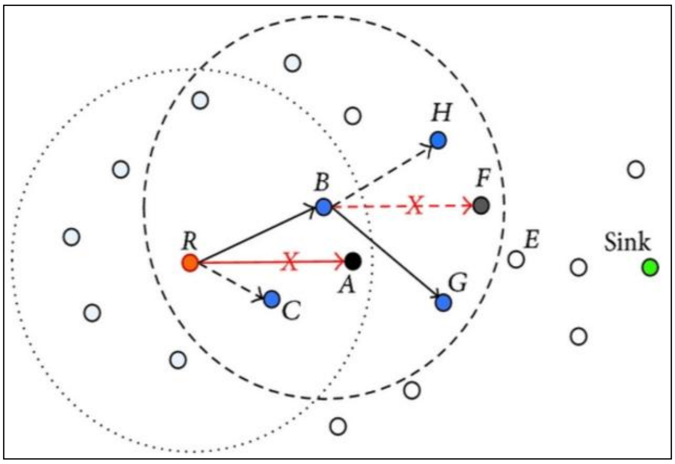


Figure 2: GRayhole Attack

III. PROBLEM INVESTIGATION

The study of complete problem routing protocols conclude that routing protocols are vulnerable for routing disruption attacks. Such kind of attack may apply due to vulnerability of routing protocol and absence of inadequate security measures. AODV doesn't have such kind of features and it is vulnerable for various security threats. Such kind of attacks not only drops the packets and degrades the performance but also compromise the integrity of communication.

The study of related existing solution address that small work has been to overcome such attack but are not adequate to overcome the impact. They can detect the malicious node but not identify the difference between trusted node and attacker node.

AODV is the one of the useful reactive routing protocol which not only helps to discover route but also maintain routing table for every route path. For security purpose it has vulnerabilities and it is easily manipulate by malicious node to destroy its network routing.

The purpose of this study is to detect Gray-hole attack in the MANET. Application of MANET such as military battle field is used to transmit the confidential data via wireless medium. Mobile Ad-Hoc Network is also used in national security applications such as monitoring and tracking the borders, nuclear attacks detection etc. The data in MANET applications is very important and due to the hostile environment of applications, Mobile Ad-Hoc Network needs security mechanism.

The objective of this thesis 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 a threshold, then that node is isolated from the network as other nodes do not forward packets through the suspected malicious node.

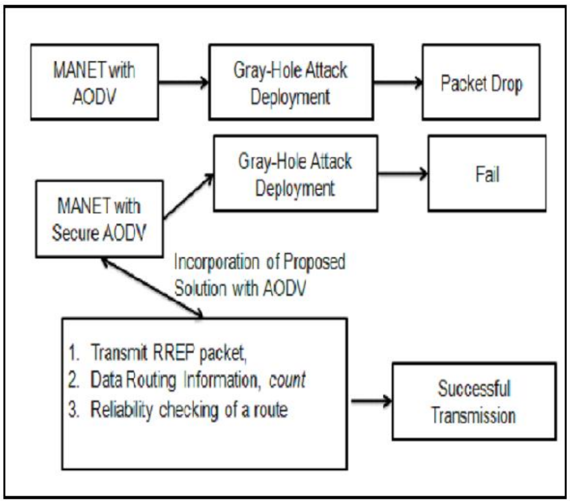
A. *The Proposed Algorithm*

In this section the proposed mechanism for defending against Gray-hole attack is presented. The mechanism modifies the AODV protocol by introducing three concepts,

1) Transmit RREP packet,

2) Data Routing Information, count

3) Reliability checking of a route


MANET with AODV
Gray-Hole Attack Deployment
Packet Drop
Gray-Hole Attack Deployment
Fail
MANET with Secure AODV
Incorporation of Proposed Solution with AODV
1. Transmit RREP packet,
2. Data Routing Information, count
3. Reliability checking of a route
Successful Transmission

V. RESULT ANALYSIS

Table 1 & 2 demonstrates the evaluated performance of normal AODV, AODV with wormhole attack and modified AODV with improved performance.

Table 1: Performance evaluation of various Scenarios in Stationary State

	20 Nodes			30 Nodes			40 Nodes		
	N	G	P	N	G	P	N	G	P
Throughput(b/s)	60	30	32	79	10	30	86	16	31
PDR (%)	66	33	33	87	0	33	96	18	35
E2E Delay	38	26	28	80	71	70	23	75	46

N: Normal State G: Gray-Hole Attack P: Prevention Technique

Table 2: Performance evaluation of various Scenarios in Mobile State

	20 Nodes			30 Nodes			40 Nodes		
	N	G	P	N	G	P	N	G	P
Throughput(b/s)	88	30.	32	90	16	20	91	30	51
PDR (%)	98	33	35	99	0.6	11	99	33	55
E2E Delay	19	55	50	90	16	96	11	70	98

VI. 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] Mozmin Ahmed, Md. Anwar Hussain "Performance of an IDS in an Adhoc Network under Black Holeand Gray Hole attacks", In proceedings of IEEE Xplorer.

[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.