An Analysis of Gray-hole Attacks on Mobile Ad-hoc Networks

Kusumlata Sachan
M.Tech, Computer Science &Engineering
SAIT Collage
Indore, (M.P.) India

Manisha Lokhande
Associate Professor, Department of CSE
SAIT Collage
Indore, (M.P.) India

ABSTRACT
Wireless communication is used to establish dialog among nodes and correspondence information. Mobile ad-hoc network is a collection of mobile nodes deployed with special purpose. Open nature of communication makes it vulnerable for various security threats. Subsequently, routing protocols are used to establish communication between nodes using route discovery mechanism. This paper gives brief details about security threats and AODV routing protocols along with gray-hole attack to investigate the need of preventive mechanism for better performance.

Keywords
MANET, Security, AODV, Grayhole, DSR, NS2.

1. INTRODUCTION
Mobile ad-hoc network is assortment of self-configurable mobile nodes along with infrastructure-less topology that are connected without wires [15]. 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 [17, 18].

The major challenge to build such network is to maintain the connection without any interrupt in network. In MANET, every node can forward packet to next hop and manage route traffic [11]. Such network may work independently or they may connect to large network such as internet [11]. The result build it dynamic and extremely climbable, versatile resolution for connect one another. Open nature of communication makes it vulnerable for numerous security threats and malicious attack might attempt to compromise the communication. Thus security is the major challenge [16].

Mobile Ad hoc Network (MANET) are most widely used network around the globe. It has strong capability to connect with other networks also. In case of security attack, there may be possibility that such network may drop the privacy of information communication. Without any proper security solution, the node that is malicious in the network will act as a normal node and it will cause eaves dropping and this type of selective forwarding attack generally known as gray-hole attack.

MANETs are vulnerable for various security threats which may include active or passive approach [8]. It may include eavesdropping, interfering, DDOS, wormhole, Gray-hole attack etc. [9, 10]. All such attacks not solely decide to compromise the privacy of communication however additionally degrade the performance by dropping the packets. The foremost essential drawback with such network is vulnerability in routing protocols. Most of the routing protocols square measure designed as per resource constraint and higher performance throughout wireless scenario. None of them is meant with security policy and keep knowledge or node safe from alternative malicious nodes [8].

In this manner, Gray-hole attack is one in each of the severe security threats that not exclusively compromise the protection of network but to boot degrades the performance by dropping the packets [3]. A collection of nodes is also compromised in such the simplest way that it should not be doable to notice their malicious behavior simply. Such nodes will generate new routing messages to advertise non-existent links, give incorrect link state info, and flood different nodes with routing traffic. One in all the wide identified attacks is that the grey Hole Attack. It's the variation of region attack. Region attack is one in all the protection threat within which the traffic is redirected to such a node that truly doesn't exist within the network which node drops the whole packet. However in Gray-Hole attack, nodes can drop the packets by selection. What is more, black-hole [18] is that the ensuing threat of hollow attack on network and transport layer, wherever malicious node misguides the supply node by victimization shortest path attraction. The entire study concludes that hollow attack, Black-hole attack and Gray-hole attack lies in same class however having completely different injury mechanism [8]. Gray-hole attack is launched by single malicious node or hand in glove by a collection of malicious nodes [15].

Among the varied protocols offered AODV is most at risk of such attack. In AODV each mobile node maintains a routing table that stores succeeding hop node info for a route to a destination node [13]. Once a supply node desires to route a packet to a destination node, it uses the required route if such a route is obtainable in its routing table. Otherwise, the node initiates a route discovery method by broadcasting a Route Request (RREQ) message to its neighbors [1]. Intermediate nodes update their routing tables once they receive a RREQ message for a reverse route to the supply node. All the receiving nodes that don't have a route to the destination those nodes broadcast the RREQ packet to their neighbors. Nodes that are Intermediate nodes they increment the hop count and after that they forwarding the RREQ. A Route Reply (RREP) message is shipped back to the supply node once the RREQ question reaches either the destination node itself or the other node that contains a current route to the destination.

Jaydeep et al. [7] planned a mechanism to notice gray-hole attack by choosing alternate path towards the last word destination. They conjointly planned a method to stop ad-hoc network from this dangerous attack victimization alarm message and bypass malicious node. So as a result of irregular behavior of gray-hole attack, it's advanced task to notice and forestall throughout communication. Technique planned in this paper increase the protection mechanism and responsibility issue of detective work malicious node by

proactively involving the neighbor nodes of a malicious gray-hole attack [7]. We tend to found the concept planned by author fascinating and that we have determined to implement the rule planned by him and conjointly attempt to improve the network performance.

The planned work can produce network situations with multiple mobile nodes to make, notice and forestall gray-hole attack [5].

2. RELATED WORK

The study of complete work concludes that varied authors have investigated regarding security threats and conclude that it is one among the severe security attack could also be apply through exploring the weakness of routing protocols. Such types of attacks are called routing disruption attacks. A study of relevant analysis paper concludes that also there's scope to analyze the answer to avoid gray-hole attack.

Sukla Banerjee [6] planned a mechanism for detection/removal of grey hole attack along with cooperative black attack in mobile ad-hoc networks. In this mechanism rather than causing the full information traffic at a time it divide the full traffic into some little sized blocks. In order that malicious nodes are often detected associate degreed removed in between the transmission of 2 such blocks by guaranteeing an end-to-end checking. Supply node sends a prelude message to the destination node before begin of the causing any block to alert it regarding the incoming information block. It is time overwhelming rule it takes time in changing of total traffic into little sized blocks.

A Rajaram[8]proposed malicious node detection system for MANET. In this mechanism they proposed a trust system. Trust based packet forwarding scheme for detecting malicious nodes using routing layer information. It uses value to favour packet forwarding by maintain a trust counter for each node. When MAC layer security protocol attaining low delay, highly speed it achieves high packet delivery ratio. If the trust counter vale falls below a trust threshold the corresponding intermediate node is marked as malicious.

Mechanism for detection of grey hole attack in mobile impromptu network are planned by Jaydip et al. [5]. They planned a mechanism to sight associate degreed defend the network against such an attack which can be launched hand in glove by a group of malicious nodes. The planned security mechanism will increase the responsibility of detection by proactively invoking a cooperative and distributed rule involving the neighbour nodes of a malicious grey hole node. Detection call works on associate degree rule supported threshold cryptography. Simulation results show that the mechanism is effective and economical with high detection rate and really low false positive rate and management overhead.

Qutaiba razouqi [13] proposed simulation performance DSR&MANET routing protocots.This method have better performance AODV by metrics examined. AODV maintained high speed and average energy consumption, reliable but traffic in alternate class between CBRand VBR. This method is only CBR main successful work.

Arjun chaudhary[11] proposed a new multi hop cooperative protocol for dynamic traffic pattern selective MANET by using NS2. In this he explains behaviour packet size changes with the time interval. These work help devoted to optimize the packet delivery ratio for high node density when using dynamic traffic pattern. Performance matrix used for analysis of network NS2 performance by throughput. Dynamic traffic in node communication ensures high packet delivery multihoc communication based higher throughput these depend on density of node for dynamic traffic pattern.

Parineet D.Shukla[16] proposed detection of gray hole attack in mobile Ad hoc network (MANET) and defined the network against such an attack which may be launched detect malicious node in the particular network. This algorithm use malicious node in the respective path can be detected analytically performance can be improved .it is based on router theory, packet forwarding and behaviour of particular node. Algorithm by use easily router path find and simple send request massage so that processes time consuming. Second phase in given formula can be check packet dropping each node then increase performance of the network.

Shani makwana[4, 12, 15] proposed detection &elimination of grayhole attack using dynamic based technique in MANET. These help to solve MANET security challenge problem. The proposed algorithem based on parameters throughput, PDF and end to end delay are compared with the AODV protocol having gray hole attack.

3. AD-HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL (AODV)

AODV is a reactive routing protocol that is intended for ad hoc networks. Ad-hoc networks are temporary kind of network deploy for special purpose. AODV is on-demand protocol specially designed for temporary network. This can be suited for dynamic self-configured networks such as ad-hoc network [13]. AODV provides a loop free paradigm along with strategic route management for broken links. AODV has very low bandwidth requirement and AODV has low overhead comparatively less than other protocols because AODV does not require periodic route advertisements.

4. SECURITY THREATS / ATTACK

The open nature and low cost of implementation of wireless ad-hoc network make them prone to various security attacks [1].

Also, it is mostly deployed in unfavorable environment that leads in worsening the safety aspects of network. Thus, before setting up the network it is very much needed to ensure that there exists a secure path between nodes involved in communication. The security becomes even a major concern as the network grows [2, 9].

Majorly, there are four security goals also called as primary goals that needs to be addressed in ad-hoc networks viz-

1. Confidentiality- It refers to protecting the message from a passive attacker so as to maintain the secrecy of message.
2. Integrity- This refers to ensuring that the message was not altered, changed or tampered while in transit. It should be received as it was sent originally by the sender.
3. Authentication- It impose check at the origin of the message that is it makes sure that the message is actually from the sender which it claims to be from.
4. Availability- This is the surety of network resources and network services being available as and whenever required by the legitimate users of the network.

Data freshness is also one of the aspects of security issues which imply that the data being sent by the sender is recent and not the older copies.

Generally, there are two types of attacks regarding security in networks that are active attack and passive attack [9, 10].

Passive attack - It is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is slowly to gain information about the target and no data is changed on the target. In passive reconnaissance, an intruder monitors systems for penetrability without interaction, through methods like session capture.

Active attack - It is a network exploit in which a hacker attempts to make changes to data on the target or data in route to the target.

Types of active attacks:

1. Masquerade attack - The intruder pretends to be a particular user of a system to gain access or to gain greater facility than they are authorized for. A masquerade may be attempted by using the stolen login IDs and passwords, through bypassing the programs/code for authentication mechanism or through finding security gaps.
2. Session replay attack: A hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.
3. Denial of service (DOS) attack: Users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle [14].

5. GRAY-HOLE ATTACK

A gray-hole attack is next level of black-hole attack used to bluff the source and monitoring system by partial forwarding. In gray hole attack, attackers uses selective data packet dropping method to behave as genuine node and try to participate into full communication [9]. Gray-hole malicious node takes part into route discovery process and then updates the source route routing table or cache as shortest path [3, 8]. Afterwards, source always consider malicious node as next hop node and forward packet to same. Node which is malicious captures all the incoming packets but drop on random basis. This complete process creates makes toughness against prevention and detection mechanism because nodes can drop packets partially; this drop may not be possible only due to its malicious nature but it may happen also due to overload, congestion or selfish nature of the node. 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 normal to malicious by behaving genuine to sinkhole. Gray hole attacked node can act as normal node switch over to malicious node, thus it becomes too complicated to identify the state whether mode is normal node or malicious node.

In the ad-hoc on demand distance vector routing it process every node and each node carry a routing table. This routing table have ultimate destination and next hop information. This information is used to discover route from source to destination. AODV nodes check routing table to know that if 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 hare listed below;

5.1 Phase 1

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.

5.2 Phase 2

It is the implementation phase of gray-hole attack. In this phase 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 and act as normal node with sending the packets. Thus, sometime it transfer packet and sometime malicious node drop the packets. When a node is in the state of malicious node it also forwards some packet and this 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 selective dropping representation in block.

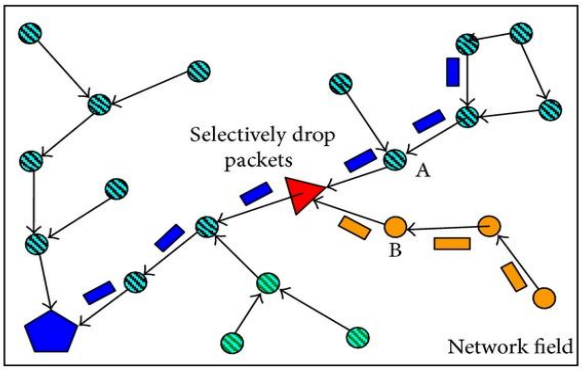

Fig 1: Selective Dropping

6. CONCLUSION

The complete study concludes that Gray-hole attack is one of the most severe security threats in ad-hoc network which happen due to vulnerabilities of AODV routing protocols. Various authors performed study about the same and investigate that such attack explores the weakness of routing protocols and attempt to disrupt the network communication. This paper perform study about various security threats, gray hole attack and AODV routing protocol and concludes that there is need to develop a security solution for AODV routing protocols to avoid security threats and prevent communication. These phenomena will avoid performance loss and help to increase successful transmission.

7. REFERENCES

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

[2] 2. Yinghua Guo,Sylvieb Perreau,Trace flooding attack in mobile Ad hoc networks IEEE 2007.

[3] 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.

[4] 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.

[5] Jaydip Sen, "An Analysis of Routing Disruption Attack on Dynamic Source Routing Protocol." IEEE, 987-1-4577-0787-2/11, 2011.

[6] Sukla Banerjee "Detection/Removal of Cooperative Black & Gray Hole Attack in MANETs" in proceedings of the World Congress on Engineering & Computer Science 2008.

[7] 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.

[8] A. Rajaram,Malicious Node Detection System for Mobile Ad hoc Networks,in proceeding of the International jounaral of computer science &information Technologies 2010.

[9] Minda Xiang,Yu chen,Wei Shinn Ku,Zhou su,mitigating DDOS attacks using protection nodes in mobile Ad hoc networks,pub in IEEE 2011 proc.

[10] V.Shanmuganthan ,Grayhole attack in MANET publish IRACST vol 2,Dec2012.

[11] Arjun Chaudhry,Improving Performance of MANET via Cooperative Communication with Selective Cooperation method considering Dynamic Traffic Pattern using NS2, published in IEEE , 978-1-4799-5958-7/14,2014.

[12] S.Sreenvasa chakrarthi, Intrustion detection tech.&Instrusion detection system in manet 6th international confrance on computation Intelligance and communication networks 2014.

[13] Qutaiba Razouqi,Extensive Simulation Performance Analysis for DSDV, DSR and AODV MANET Routing Protocols, Published IEEE, 2013.

[14] Yoguandhara Patil,Comparison of Mechanisms against Denial of Service Attack in Mobile Ad-Hoc Networks, publish IEEE 2015.

[15] Shani Makwana, Cooperative Gray Hole Attack Detection and Prevention Techniques in MANET,Published International Journal of Science and Research (IJSR),Jan 2015.

[16] Parineet D Shukla,An Analytical Approach for Detection of Gray Hole Attack in Mobile Ad-hoc Network (MANET).IEEE,978-1-4799-3975,2014.

[17] Vishali Mittal International "Prevention and Elimination of Gray Hole Attack in Mobile Ad-Hoc Networks by Enhanced Multipath Approach, Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Issue 5, May 2015.

[18] Arshdeep singh, Detection and Prevention of Black Hole Attacks in Manets Using NTP Method, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, February 2016.