Survey of Grey Hole Attack and Its Impact on Reactive Routing Protocol in Mobile Ad-hoc Network (MANET)

[1]Aditya Kumar,[2]Anurag Vishwakarma,[3]Prasanna Dwivedi
[1] Assistant Professor,[2] Scholar,[3] Scholar
[1] Department of Information Technology,
[1] Shri Shankaracharya Engineering College, Bhilai, India

***Abstract*— A Wireless Ad-Hoc Network (WANET) or Mobile Ad-hoc Network (MANET) is decentralized type of wireless network. This network is Ad-Hoc because it is infrastructure less network. Wireless mobile Ad-Hoc network are configured by itself, hence it is also a dynamic network which means nodes can move, join network or remove itself from network anytime and anywhere.The most famous technology is Mobile Ad-hoc Network which contributes in various fields.[1] It is having multiple/variable number of mobile nodes. Its main key for becoming popular is less cost, energy efficiency and simpler use. Becoming MANET as a famous technology hence also increases the chance of attack. Greyhole attack is one of the scariest attack which affects the working of routing protocol. In this attack the selectively dropping and forwarding of packets by the attacker node take place. This research paper is about the study of grey hole attack. [2]**

***IndexTerms*—AODV, DSR, Grayhole Attack, MANETS.**

I. INTRODUCTION

MANET's one of the most famous technology which contributes towards various fields. In this network it's consist of various mobile nodes which is not having any infrastructure and is connect in wireless manner. Each node may continue or discontinue its contribution towards the network at any time. The nodes which we are talking about are acted as a router. We cannot predict the path of transmission of as it is highly unpredictable,and it is not static hence it is dynamic in nature. So, it is having many vulnerabilities into security measures[3]. It is also very useful for this character too. This paper is the study of famous routing protocol AODV (Ad-hoc On-demand Distance vector) are under Greyhole attack in MANET's. Grey hole is the example of network layer attack.

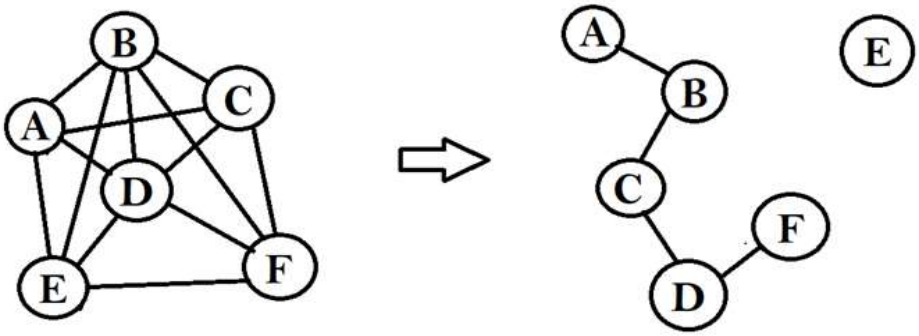


Fig 1. Nodes in MANET Network

II. ROUTING PROTOCOL

Generally, routing protocol are of three type that is reactive, proactive and hybrid. Proactive protocols are those protocol in which topologies which is having different node maintain one or more table which represent the entire network. These tables contain routing information from each to every node and hence updated regularly. Examples are OLSR, DSDV, and B.A.T.M.A.N..

Reactive protocol is on demand bandwidth efficient routing protocol of mobile ad-hoc network. This protocol has two main route discovery and route maintenance. Examples are AODV, DSR, and ABR [4]..

Hybrid routing protocol is basically, a combination of advantages of both proactive and reactive protocol. Examples of this type of protocol are ZRP, ZHLS.

III. Disadvantages of Routing Protocol and Table Form

Table 1. Disadvantages of Proactive, Reactive and Hybrid Routing Protocol

Proactive Protocol	Reactive Protocol	Hybrid Protocol
Maintenance requires respective amount of data. Reaction is not faster in restructuring and failures.	Latency time is high in route finding. Network clogging is possible on excessive flooding.	No. of nodes which are activated decides it's advantage. Traffic demand's reaction is dependent on gradient of traffic volumes.

IV. Ad-Hoc On Demand Distance Vector (AODV)

One of the most famous reactive protocol is AODV. It is based on distance vector routing algorithm. It is on demand reactive routing protocol hence it routes only when needed. It uses hop to hop routing and every node carries it's routing table with sequence number of each routing information. [4] Every node updates it's routing table whenever it receives control message, it uses sequence number and hop count for updating a routing table. The following control messages used by AODV are:

HELLO Message

Detection of link and monitoring is done by every node periodically by broadcasting a HELLO message. It is used to know the neighbor nodes.

RREQ (Route Request) Message

When any source node wants to convey a message or data it first broadcast a RREQ (Route Request) packets in the network. This message includes the source address, destination address, source sequence number, destination sequence number, request ID and hop count

RREP (Route Reply) Message

A node which has valid destination link or destination node when receives RREQ then it unicast RREP (Route Reply) to the source node. It contains the source address, destination address, destination sequence number, lifetime and hop count.

RERR (Route Error) Message

Every node monitors its neighbor node. Whenever any node detects a link with next node is broken it unicast RERR (Route Error) message which contain unreachable destination address and unreachable destination sequence number [4].

V. Working of AODV

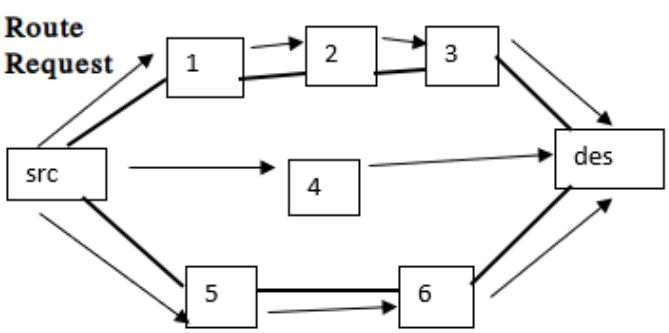
Working of AODV reactive protocol are in two phases route discovery and route maintenance. Whenever any node has any data to transmit then that node checks it's routing table to search out weather it has any route to destination or not. If yes, it has route then node transmit its data to another node otherwise it first starts route discovery..

Route Discovery

In this phase, the route reply was send by source node to its neighbors. Routing table is checked by each intermediate node when it receives a RREQ (route request) to determine the route towards its destination node. When it found route to destination then it sends RREP (route reply) and if it unable to find route then it rebroadcast the RREQ to its neighbor [6]. Here are some figures to demonstrate this phase how its work.

Route Maintenance

In this phase, every node periodically broadcast HELLO message for local connectivity. It assumes that the link break to the neighbor and upstream node notify the source node with route error message (RERR) which contain the unreachable destination address as well as entire route based on the nodes is nullify if the node does not receive any node from a neighbor node during a few second then it again performs route discovery phase [7].



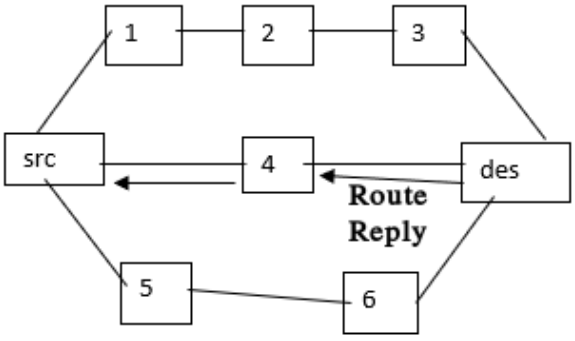


Fig 2. Route Request **Fig 3. Route Reply**

In above two figures" src" refers to source node and des refers to destination node and numbers are intermediate node. Fig 1 demonstrate how RREQ is broadcast by source node and fig 2 shows how RREP unicast by destination node. Src node sends RREQ to every node but RREP is selected on basis of which route having a shortest path

VI. GRAYHOLE ATTACK ON AODV

This attack takes place on Ad-Hoc networks. Gray hole attacker nodes have capabilities to hide themselves. When the data packets are received by malicious node, instead of forwarding them all, that selectively drops certain packets [8]. Selective dropping of packets can be done either on single IP address or on the range of IP addresses.

A Routing Table is maintained by every node in the network which is used to store the information of the next hop node. To route the packet from source to the destination node, the source node performs a check about a specific route in its routing table. [9] In case the route is found in the routing table, the packet is sent to the next node. Otherwise, *Route Request* (RREQ) message is broadcasted by the nodes to their neighbor nodes. After receiving *Route Request* message, the routing table of the intermediate nodes are updated for reverse route to broadcasting (source) node [10].

After receiving the RREQ query either by destination node or intermediate nodes having route to destination, a *Route Reply* (RREP) message is sent back to the source node. There are two main stages to plate a gray hole attack

1. In first stage, a malicious node calls itself a valid and shortest route to destination node. This is intended to interrupt data packets in the false route.

2. The second stage is the implementation stage of gray-hole attack, the interrupted packets are dropped with certain probability. The behavior of the attacker node is changed rapidly, due to this behavior it is hard to find out in the network [11] [12].

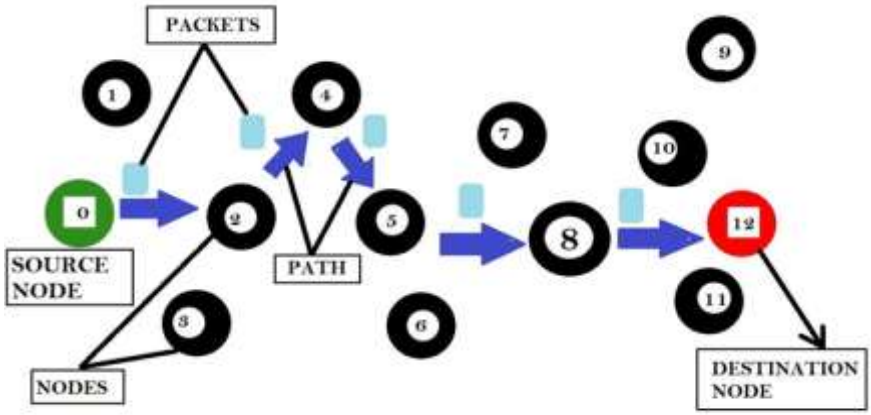


Fig 4. Normal Communication (When no attacker node is present)

The above figure 4 illustrates the condition, in which no attacker node is present. In this condition, source node is sending the route request and the route reply is been sent by all the intermediate nodes present between source node and destination node. Once the path between source and destination node is established, source node starts sending data packets to destination node.

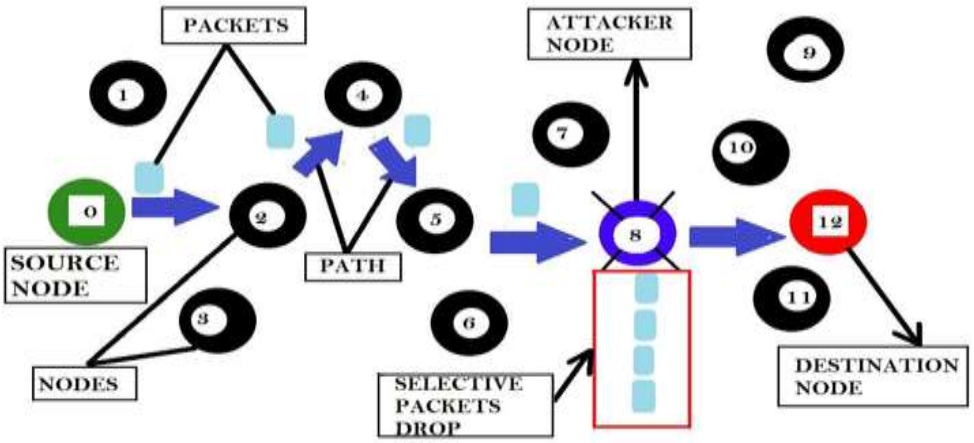


Fig 5. Gray Hole Attack

Whereas in above fig 5, node 8 is a Greyhole (attacker) node. The attacker node get involved in the path of communication by sending false hop count and route reply message. When source node sends data packets to the destination through intermediate nodes, the attacker node present in the path starts dropping data packets selectively and sends false acknowledgement to the destination node.

The malicious node can switch to normal at times, due to this capability of the attacker node it is very hard to detect and prevent the attack on the network. Grey Hole attack is also termed as node misbehaving attack. There are three ways in which the grey hole attack can occur:

1. On basis of the origin of message - In this type, the malicious node drops the only packets which comes from some particular nodes.
2. On the basis of packet type - In this way, attacker node drops the packet on the basis of the type of the packet that is, either a Control Packet or a Data Packet.
3. It can also dropped randomly - any one of the above methods can be applied. The attacker node can drop the packets either on the basis of source (origin) of the message or on the basis of the type of the packets on the random basis.

VII. Related Work

Chaudhari Rajashri M., PatilManesh P. [1]

proposed the mechanism for detection of Blackhole and Greyhole attackers based on Statistical-based Detection of Blackhole and Greyhole attackers (SDBG). In the suggested mechanism nodes exchanges their encountered data or information and based on that calculate the forwarding behavior. In SDBG detection scheme, nodes are evaluated by their encounters information with other nodes. Forwarding Ratio (FR) is the ratio between total number of sent and received messages in the network. If the forwarding ratio is lower than the threshold then the node is judged as malicious.

Bansi S. Kantariya1, Dr. Narendra M. Shekokar2 [6]

suggested a trust mechanism to detect the Grayhole attack. In the Trust mechanism first, we will evaluate the trust value of the node in the network which is like the theory of trust in human society and then this trust value is used to detect the malicious activity in our case packet dropping. In the suggested technique they use energy consumption and task completion as the parameters for calculating the trust value. An attacker node can manipulate its attacking strategies to avoid itself from being detected and this mechanism has also taken care of such situation for Grayhole detection.

Shaiffu, Amandeep Kaur Virk [9]

Proposed a mechanism which adopted a hybrid trace-back approach in which packet marking and packet logging are integrated for detection of Grayhole attack.

In the suggested hybrid scheme for detecting Grayhole, it deploys both packets packet logging and marking scheme in the router. When packets come with to the router, it checks the number of hop count in the IP header to decide to conduct marking or logging. In the single scheme approaches, the routers can do a single trace back task without judging. However, the overhead is accountable. However, the routers in hybrid scheme can reduce plenty of storage overhead. Therefore, the trade-off is reasonable and meaningful.

In the suggested mechanism hybrid approach detects and eliminates the Grayhole attack effectively with better throughput, delay, load and jitter.

Geetanjali Rathee and Hemraj Saini [10]

Proposed a mechanism for detection of Grayhole attack and ensure the security against Grayhole attack by calculating the packet delivery percentage of every node and if the node having less percentage of packet delivery than the predefined threshold value (i.e. 97%) is considered as grey hole or malicious node. In this approach 2-hop preceding node phenomenon is used which immediately select another route to re-route the packets of data to recover from against the Grayhole attack. In NS2 simulator this approach is analyzed simulator beside different network metrics over static and dynamic environments having scalable size of network.

IX. Conclusion

A wireless ad hoc network (WANET) or MANET is one of the most popular technology because of its speed, cost effective etc. and emerging in various field. As the popularity of wireless network increases, chances of different types of attack on a wireless network is also increases. In this paper we studied about Grayhole attack and protection of data and network most important concern when such attack occurs. We must use secure cryptography schemes to protect data because if malicious node would be able to gain access on data packet the can't read/understand it as well as to secure network sophisticated routing protocol and effective algorithms need to develop for secure network.

References

[1] Chaudhari Rajashri M, Patil Manesh P, "Performance Evaluation of Attack Detection Algorithms in Delay Tolerant Networks", International Journal of Computer Applications (0975 – 8887) Volume 171 – No.4, August 2017

[2] Rupinder Kaur, Parminder Singh, "Black Hole and Greyhole Attack in Wireless Mesh Network", American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-3, Issue-10, pp-41-47 www.ajer.org

[3] Wikipedia, "Ad-Hoc Routing Protocols", https://en.wikipedia.org/wiki/List_of_ad_hoc_routing_protocols

[4] Aditya Kumar, Aakanksha S. Choubey, "Detection of Sinkhole Attack based on Analysis of Routing Behavior in an AODV Routing Environment", IJSRD - International Journal for Scientific Research & Development| Vol. 3, Issue 04, 2015 | ISSN (online): 2321-0613
[5] Rupali Sharma, "Gray-hole Attack in Mobile Ad-hoc Networks: A Survey", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1457-1460
[6] Bansi S. Kantariya, Dr. Narendra M. Shekoka," Detection and Mitigation of Greyhole Attack in Wireless SensorsNetwork Using Trust Mechanism", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438
[7] Kanu Geete, Piyush Kumar Shukla, Anjana Jayant Deen," A Survey on Grey Hole Attack in Wireless mesh Networks", International Journal of Computer Applications (0975 – 8887) Volume 95– No.23, June 2014.
[8] N.Bhalaji, A.Shanmugam, "Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Ad-Hoc Networks", International Conference on Communication Technology and System Design 2011, online at www.sciencedirect.com
[9] Shaiffu, Amandeep Kaur Virk, "Greyhole and Blackhole Attack Identification and Prevention using IP Backtracking in WSN", International Journal of Computer Applications (0975 – 8887) Volume 169 – No.5, July 2017
[10] Geetanjali Rathee and Hemraj Saini, "A SECURE MULTICAST ROUTING PROTOCOL AGAINST GREY HOLE ATTACK", ARPN Journal of Engineering and Applied Sciences©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved. VOL. 11, NO. 21, NOVEMBER 2016
[11] Munish Wadhwa, Ashwani Sethi, "A Review on Various Kinds of Attacks in MANET", IJCSN International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017ISSN (Online) : 2277-5420 www.IJCSN.org Impact Factor: 1.5
[12] Onkar V.Chandure, V.T.Gaikwad, "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", International Journal of Computer Applications (0975 – 8887) Volume 41– No.5, March 2012
[13] Rupinder Kaur, Parminder Singh, "Black Hole and Greyhole Attack in Wireless Mesh Network", American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-3, Issue-10, pp-41-47
[14] Informit, "Your Home Network: Should You Go Wireless?", https://www.informit.com/articles/article.aspx?p=101591&seqNum=2
[15] WIKI2, "Wireless ad hoc network", https://wiki2.org/en/Wireless_ad_hoc_network