IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue5)

Available online at: www.Ijariit.com

Review on Grey-Hole Attack Detection and Prevention

Suman Brar[1], Mohit Angurala[2]

Department of Computer Science and Engineering, GCET, Gurdaspur- 143521

***Abstract*— These Grey Hole attacks poses a serious security threat to the routing services by attacking the reactive routing protocols resulting in drastic drop of data packets. AODV (Ad hoc on demand Distance Vector) routing being one of the many protocols often becomes an easy victim to such attacks. The survey also gives up-to-date information of all the works that have been done in this area. Besides the security issues they also described the layered architecture of MANET, their applications and a brief summary of the proposed works that have been done in this area to secure the network from Grey Hole attacks.**

***Keywords*— greyhole, Manet, AODV, attack.**

I. INTRODUCTION

Mobile ad hoc networks (MANETs) have become important in increasingly large range of applications, such as disaster recovery, rescue mission, tactical battlefield, mining operations, maritime communications, vehicle network, casual meeting, and campus network and so on. A Mobile ad hoc network (MANET) is a self organized system which doesn't have any pre-defined network infrastructure where mobile devices are connected by wireless links.

As we all know MANETs are more vulnerable to various attacks, all these three layers i.e. Physical MAC and Network layer suffer from different attacks and it cause routing disorders. The different kind of attacks in the network layer varied such as selective forwarding attack and modifying some parameters of routing messages.

Black Hole and Grey Hole Attacks

Black hole means incoming and outgoing of information is dropped, without telling the source node that the information did not communicate with planned receiver node. Black hole attack as its name specifies that, the attacker attacks and discards the whole packets from receiver node. A black hole node done its job in the following strategies: one time RREQ(route request) and RREP(route reply) message is received by source node ,then attacker send RREP message directly and shows that it is real receiver node.

Grey hole attack is the kind of denial of service attack. In this attack, the router which is mesh behave just not well and a subset of packets are forward and handle by receiver but leave by other network. Black hole and Grey hole attacks are the two traditional attacks under wireless mesh network which spoil the network topology and degrade the network performance.

GRAY HOLE ATTACK, A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are 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 [9]. 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 [10]. 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.

Grey hole attack will carry a large price of effect to the performance of wireless mesh network. In multiple ways the false behaviour may exhibits by Grey hole attack, Grey hole attack is a node which react maliciously for some specific time duration by releasing packets but may come to balanced behaviour and later forward the packets through packet ID to other packet. A Grey hole may also behave a random behaviour by which it rejects some the packets randomly when it forward to other packets. Thereby its detection is even more difficult than black hole attack.

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 behaviour [8]. Both normal node and attacker are same. Due to this behaviour it is very hard to find out in the network to figure out such kind of attack. The other name for Gray hole attack is node misbehaving attack.

II. Literature Review

Gupta [2015] proposed a new method RTMAODV (Real Time Monitoring AODV). It does not introduce any overhead. Moreover neighbor node detects and prevents Grey Hole attack using real time monitoring. The concept of broadcasting is being used in the method. Node which replies to Route Request (RREQ) by source is being monitored in promiscuous mode. Detection of malicious node is actually done by neighbor node of Route Reply (RREP) sender node i.e. suspected node.

Ranjan, Singh & Singh [2015] have focused on the Grey Hole attacks. These Grey Hole attacks poses a serious security threat to the routing services by attacking the reactive routing protocols resulting in drastic drop of data packets. AODV (Ad hoc on demand Distance Vector) routing being one of the many protocols often becomes an easy victim to such attacks. The survey also gives up-to-date information of all the works that have been done in this area. Besides the security issues they also described the layered architecture of MANET, their applications and a brief summary of the proposed works that have been done in this area to secure the network from Grey Hole attacks.

Gupta & Rana [2015] surveyed regarding the various kind of attacks happened on the network layer in MANET. The proposed scheme has been given for securing the network in malicious environment. In this source node will start the route discovery for data transfer like as AODV default process. In next step, all possible paths to reach destination in routing table and all information about the all path which is available for data transfer has been stored. Then the path having highest sequence number will be deleted from the routing table. Here they have deleted first two paths having highest sequence number and then the data will be sent to third highest path. They observed that throughput and end-to-end delay decreased in all three cases of attacks as simulation time increased.

Jain & Khuteta [2015] proposed a scheme in which they deploy the base node in the network that increases the probability of detecting multiple malicious nodes in network and further isolate them from taking part in any communication. In this procedure, Base Node sends dummy RREQ packet in network with the destination set as random generated network address that do not exist in the network, and it start timer and wait for replies from other nodes. Once the timer expires, it checks for the replies received from nodes. Genuine nodes do not send reply as the dummy RREQ is for node that do not exist in network.

Arya et al. [2015] instigate to detect and avoid the wormhole attack and collaborative Grey Hole attack using trusted AODV routing algorithm. During the route discovery phase of the AODV Routing protocol, the trust value is also computed for all the neighbours of any node. To detect the malicious behaviour of nodes, in this scheme each node maintains a Trust table. The Trust table has two columns. First the identifier or name of its entire neighboring node and second its relationship status with the neighbor node that could be Most Reliable, Reliable or Unreliable.

Chaube et al. [2015] have studied the impact of network size of their proposed Trust Based Secure On Demand Routing Protocol called "TSDRP" and AODV routing protocol for making it secure to thwart Grey Hole attack. TSDRP protocol is capable of delivering packets to the destinations even in the presence of malicious node while increasing network size. In order to make result more accurate the performance of these two protocols TSDRP and AODV was tested with respect to different performance metrics and after observation of performance analysis, they concluded that in case of Grey Hole attack TSDRP demonstrate better performance in almost all parameters: PDF, AED, AT and NRL as compared to AODV.

Abdelaziz et al. [2014] have analysed all possible security attacks against ad hoc on-demand distance vector protocol, and they have given a detailed overview of each attack that can target the operation of this protocol. Particularly, they have focused on attacks that targets routing flow, such as flooding, Grey Hole, wormhole, and rushing attacks. The presented analysis in this paper is potentially helpful for protocol designers to assess their designs, and for security researchers to validate their security mechanisms such as intrusion detection systems and trust management systems.

Parmar & Jethva [2014] analysed behaviour of Grey Hole and Gray hole attacks under AODV protocol and show the effects of both on network layer. They have also tested malicious behaviour of AODV under above attacks using various performance parameters like throughput, packet delivery ratio, normalized network load and end to end delay using different simulation parameters. They also concluded that Grey Hole attack degraded the network performance in terms of packet efficiency and throughput and behaviour of Gray hole was very difficult to judge because sometime they acted as normal node but sometime they dropped selective packets.

Patel & Chawda [2014] reviewed the two most important and vulnerable attacks namely the Grey Hole and the Gray hole attacks. This paper shows how the performance of the network is degraded due to these two attacks. Many techniques to mitigate these attacks have been provided. Every technique has its own advantages and limitations which are also listed in the paper.

III. CONCLUSIONS

GREY HOLE AND GRAY HOLE ATTACKS UNDER AODV PROTOCOL AND SHOW THE EFFECTS OF BOTH ON NETWORK LAYER. THEY HAVE ALSO TESTED MALICIOUS BEHAVIOUR OF AODV UNDER ABOVE ATTACKS USING VARIOUS PERFORMANCE PARAMETERS LIKE THROUGHPUT, PACKET DELIVERY RATIO, NORMALIZED NETWORK LOAD AND END TO END DELAY USING DIFFERENT SIMULATION PARAMETERS. THEY ALSO CONCLUDED THAT GREY HOLE ATTACK DEGRADED THE NETWORK PERFORMANCE IN TERMS OF PACKET EFFICIENCY AND THROUGHPUT AND BEHAVIOUR OF GRAY HOLE WAS VERY DIFFICULT TO JUDGE BECAUSE SOMETIME THEY ACTED AS NORMAL NODE BUT SOMETIME THEY DROPPED SELECTIVE PACKETS

REFERENCES

[1] Anishi Gupta, "Mitigation Algorithm against Grey Hole Attack Using Real Time Monitoring for AODV Routing Protocol in MANET" IEEE 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom).

[2] Rakesh Ranjan, Nirnemesh Kumar Singh, Ajay Singh, "Security Issues of Grey Hole Attacks in MANET" International Conference on Computing, Communication and Automation (ICCCA 2015).

[3] Anurag Gupta, Kamlesh Rana, "Assessment of Various Attacks on AODV in Malicious Environment" 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015.

[4] Sakshi Jain, Dr. Ajay Khuteta, "Detecting and Overcoming Grey Hole Attack in Mobile Ad hoc Network" IEEE 2015 International Conference on Green Computing and Internet of Things (ICGCIoT).

[5] Neeraj Arya, Upendra singh, Sushma singh, "Detecting and Avoiding of Worm Hole Attack and Collaborative Grey Hole attack on MANET using Trusted AODV Routing Algorithm" IEEE International Conference on Computer, Communication and Control (IC4-2015).

[6] Nirbhay Chaubey, Akshai Aggarwal, Savita Gandhi, Keyurbhai A Jani, "Performance Analysis of TSDRP and AODV Routing Protocol under Grey Hole Attacks in MANETs by Varying Network Size" 2015 Fifth International Conference on Advanced Computing & Communication Technologies.

[7] Amara korba Abdelaziz, Nafaa Mehdi, Ghanemi Salim, “Analysis of Security Attacks in AODV” IEEE 2014.

[8] Martin K Parmar, Harikrishna B Jethva, “Analyse Impact of Malicious Behaviour of AODV under Performance Parameters” 2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

[9] Ankit D. Patel, Kartik Chawda, “Grey Hole and Gray hole Attacks in MANET” ICICES 2014 - S.A.Engineering College, Chennai, Tamil Nadu, India.

[10] Durgesh Kshirsagar, Ashwini Patil, “Grey Hole Attack Detection and Prevention by Real Time Monitoring” IEEE 2013.

[11] Seryvuth Tan, Keecheon Kim, “Secure Route Discovery for Preventing Grey Hole Attacks on AODV-based MANETs” 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing.

[12] Gayatri Wahane, Savita Lonare, “Technique for Detection of Cooperative Grey Hole Attack in MANET” 4th ICCCNT 2013, Tiruchengode, India.

[13] S. Sankara Narayana, Dr. S. Radhakrishnan, “Secure AODV to Combat Grey Hole Attack in MANET” 2013 International Conference on Recent Trends in Information Technology (ICRTIT).

[14] Mohamed A. Abdelshafy, Peter J. B. King, “Analysis of Security Attacks on AODV Routing” IEEE 2013.

[15] Vani A. Hiremani, Manisha Madhukar Jadhao, “Eliminating Co-operative Grey Hole and Gray hole Attacks Using Modified EDRI Table in MANET” IEEE 2013.