Analysis Of Black Hole And Gray Hole Attack On RP- AODV In MANET

Nisha, Simranjeet Kaur, Sandeep Arora
Department of Electronics and Communication Engineering
PG Student, S.S.C.E.T Badhani, Pathankot, Pb, India·
Assistant Professor, LPU, Phagwara, Pb, India[1].
Assistant Professor, S.S.C.E.T Badhani Pathankot, Pb, India[2].

***Abstract*-The wireless ad hoc network is a collection of nodes which over shared a wireless medium to communicate with each other that do not rely on predefined infrastructure. In this time of science and technology, all the technical domains are growing continuously and provide different types of communication devices and instruments. As the domain of communication, different networks are established to provide high performance and reliable end to end delivery. Today, MANET is common due to its key feature i.e. absence of central authority management agency or a fixed infrastructure. But at same time, security issues in MANETs are one of the most issues. It becomes very difficult task. There are various security issues in MANET i.e. black hole attack, gray hole attack. Wormhole attack, eavesdropping attack and information disclosure are some more common issues in MANET. Black hole attack and gray hole attack are the network layer attack that degrade the performance of network by dropping packets. This paper analyze the effect of black hole attack and gray hole attack on MANET and detection of these attacks by using IDS.**

Keywords: MANET, black hole attack, gray hole attack, IDS.

I.INTRODUCTION

A MANET is a self-configuring network that is formed by collection of mobile nodes like PDA's, laptops, mobile phones etc. without a centralized management. These mobile nodes communicate with each other and can move anywhere and anytime. These nodes are dynamic in nature and arbitrary located in such manner; it means interconnections between these nodes are frequently changing their position [1]. It is also known as multi-hop temporary network of mobile nodes that communicate with each other by wireless transmitter and receivers. Each mobile node router as well as host simultaneously. It is particularly vulnerable due to its various fundamentals characteristics such as dynamic topology , self-organization, self-configuration, open medium, distributed co-operation, lack of infrastructure and constrained capability [2],[3]. Due to its unique characteristics, it is very challenging task to develop intrusion detection system (IDS). There is no central server as well as gateway to monitor intrusion, network traffic and network functionality. Since medium is open, malicious node easily access it. In most of the cases MANET have to depend upon routing protocol.

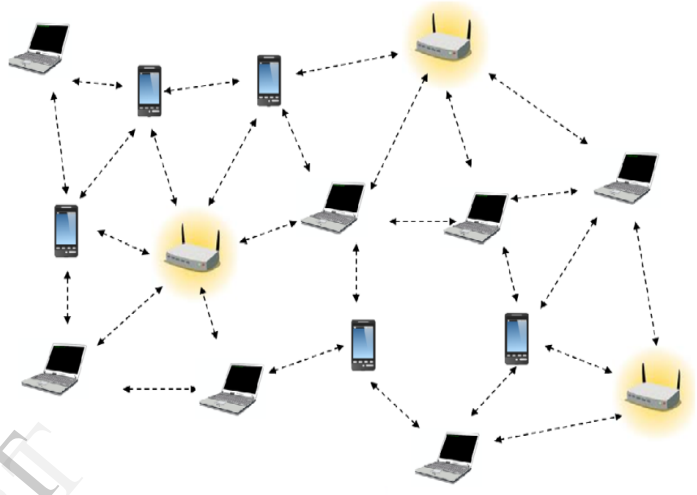


Figure 1: An example of Mobile Ad Hoc network

Routing plays an important role in provide security to whole network [4]. Routing protocols are classified into three types: proactive approach, reactive approach and hybrid approach. The most widely used RP is AODV. Because it offers good PDR and less routing overhead. MANETs are vulnerable to various types of attacks including passive attacks and active attacks. In passive attacks, attacker launched attack to steal valuable information by unauthorized listening to the network traffic. Basically, attacker snoops the data exchanged in the network without alerting it. In active attacks, attacker can use different features of the network to launch the attack. Attack attempts to modify packets, inject packets or drop packets.

II. AODV ROUTING PROTOCOL

AODV belongs to the class of distance vector (DV) routing protocol. It is one of the most popular reactive routing protocols. AODV also known as pure on-demand routing protocol because route create only when a node has data to transmit to other nodes. Due to its features life dynamic self-starting, multi-hop routing, quick aging, link breakages efficiently repaired, it most widely used in networks. AODV uses sequence number i.e. created by destination for maintaining each route entry. A requesting node always

selects that route which has highest sequence number. AODV protocol contains 3 set of message types like route request (RREQ), route reply (RREP) and route error (RRER). These messages are control messages used for establishing a path to the destination. The format of RREQ, RREP and RRER messages are shown in figure 2 and also discuss the communication between source and destination.

Type	J	R	G	D	U	Reserved	Hop count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Original IP Address							
Original Sequence Number							

(a) RREQ Packet

b) RREP Packet

(c) RRER Packet

Type	R	A	Reserved	Prefix Size	Hop Count
Destination IP Address					
Destination Sequence Number					
Original IP Address					
Life Time					

Figure 2: (a) RREQ Packet format, (b) RREP Packet format,

Type	N	Reserved	Destination Count
Unreachable Destination IP Address (1)			
Unreachable Destination Sequence Number (1)			
Additional Unreachable Destination IP Address (if needed)			
Additional Unreachable Destination Sequence Number (if needed)			

(c) RRER Packet format

When a source node wants to transmit or communicate with other node, it broadcasted RREQ messages across the network. When RREQ message received by destination, it sends back RREP message to source node only if it is destination node and route become active to the destination. When RREP message propagates back to source node then other intermediate node update their routing table as shown in figure 3. If a link breaks down while route is active then the node upstream of the break, propagates a RRER message to source node to inform it of the now unreachable destination. After receiving RRER message by the source node, it generates a new RREQ message [5]. HELLO messages are used for broadcasting information, detecting and monitoring links to neighbours.

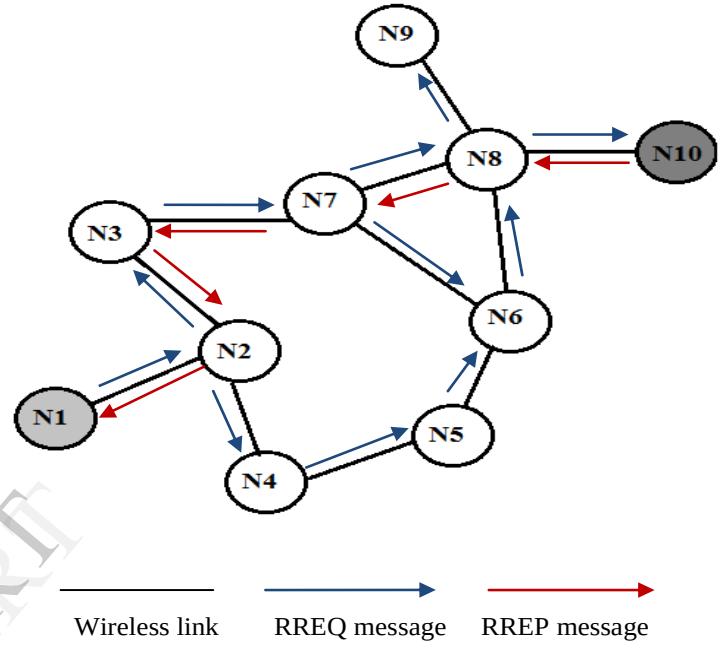


Figure 3: Route discovery process

The most distinguishing feature of AODV routing protocol to the other routing protocols is that it uses a destination sequence number to make each route entry in routing table. The destination sequence number is generated by the destination when a route is requested from it. Destination sequence number ensures loop freedom and AODV makes sure the route to the destination does not contain any loop and it is the shortest path.

III. BLACK HOLE ATTACK

Black hole attack is one of the most active DoS attack since it disrupts routing services in the network [6]. The aim of black hole attacker is to attract the network traffic towards it and advertise itself having a valid shortest path in the attention of blocking data packets. In figure 4, the source node 1 initiate's route by broadcast the RREQ message for any destination. If this RREQ packet is received by black hole node then it immediately responds with a faked RREP packet by inserting high sequence number. This message is perceived as if it coming from the destination or from a node which has a shortest as well as fresh route to the destination. Then source node gets deceived by faked RREP

packets and sends packets (data) on that route. Then black hole node instead of forwarding data simply drops [7]. This attack is called black hole attack which forms "black hole" that absorbing everything but never giving.

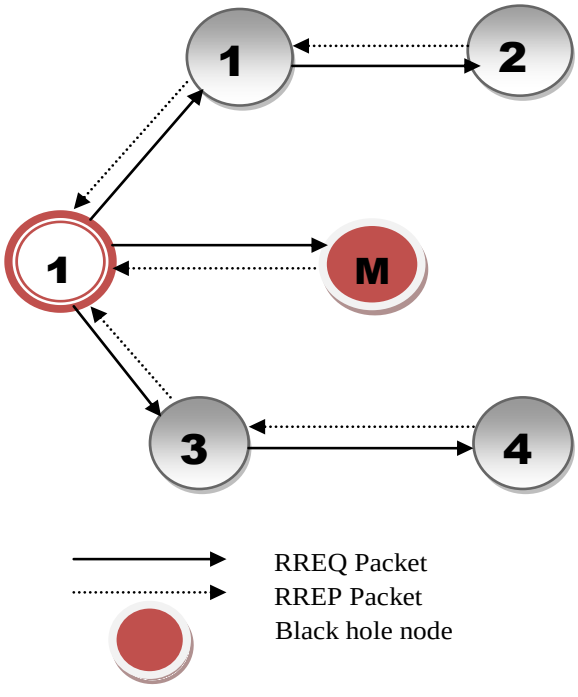
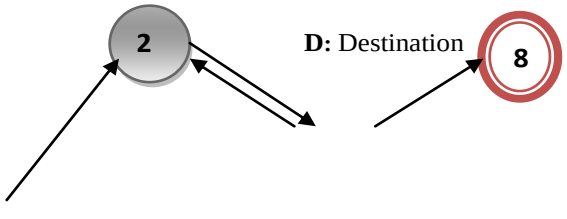


Figure 4: Blackhole attack on MANET

IV. GRAY HOLE ATTACK

The gray hole attack is also a kind of DoS attack. Gray hole attack is an extension of black hole attack in which malicious node behaviours and activities are exceptionally unpredictable. In this, malicious node advertise a same behaviour as a honest node during route discovery process and silently drops some packets or also forward packets even when no congestion occurs. This malicious node degrades the network performance that disrupts the route discovery process. This attack is difficult to detect than black hole attack. A gray hole may exhibits its malicious behaviour in various techniques. It simply drops packets coming from certain specific node in network, while forwarding all packets for other nodes. Another type of gray hole attack is a node behave maliciously for some time duration in the intention of dropping packets. This attack may also exhibit a behaviour which is a combination of above two, making detection of attack more difficult. Figure 5 describe the gray hole attack.



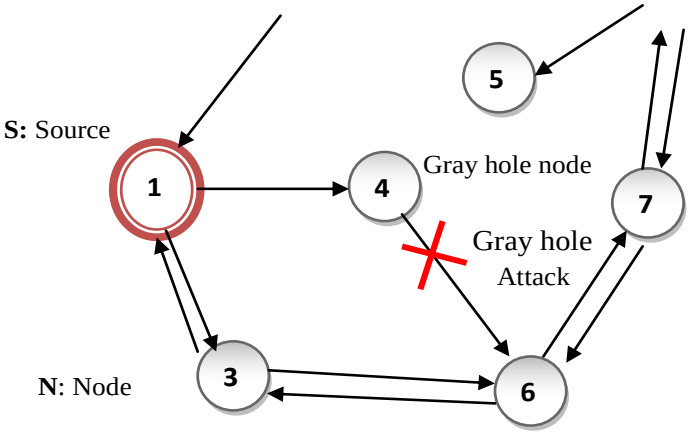


Figure 5: Gray hole attack on MANET

V. RELATED WORK ON SECURING AODV

The proposed method can be used to find the short and secured routes and prevent the black hole nodes in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP packets or not. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored in the RR-table as a first route entry. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, it means that node is the malicious node then immediately remove that entry from the RR-table.

The other proposed method for gray hole attack is the key management algorithm. This Key management algorithm based on gossip protocol to manage nodes' public key certificates. This method is very efficient and reliable. In this detection reliability is guaranteed, as evidence on forwarded packets is used. The application scope is wide, as bi-directional communication links are not necessary. The security mechanism is satisfying, as it is hard for malicious nodes to escape tracing. In this there is no need to nodes to monitor each other [9].

In [2], Detection and removing of black/gray hole attacks processes for black/gray hole attack by source node: is dividing data packets into k equal parts and forward message to destination consist number of messages. These messages are received by all neighbours of route in the network. After ensuring that destination node knows count of messages, source begins start sending of data. Timer is setting until getting number of data packets

that destination receives. If received number of packets from destination is less than a limit, that it initiates removing process of black/gray hole attack. Also if after terminating of timer, if did not receive any message from destination, then starts removing process of black/gray hole attack and also start detection process for black/gray hole attack by destination node.

In [8], P. Agarwal et al have proposed a technique for detecting a chain of malicious nodes i.e. black hole node and gray hole node in ad hoc network. In this total traffic is divided into small data blocks and initially built a backbone network of strong nodes over the ad-hoc network. These nodes are assumed be powerful in terms of radio range, computing power and also assumed trustful one. Nodes other than strong nodes considered as regular nodes. The major drawback of this approach is that some strong nodes are powerful in terms of power, antenna range but this assumption is not valid for all types of MANET. The optimality of backbone network in terms of minimality and coverage is not proved. Then this algorithm will be fail if attacker attacks on strong nodes because it violates assumption that strong nodes are always trusted nodes.

In [10], the authors proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive.

In [11], the authors analysed the black hole attack and showed that a malicious node must
increase the destination sequence number sufficiently to convince the source node that the
route provided is sufficiently enough. Based on this analysis, the authors propose a statistical based anomaly detection approach to detect the black hole attack, based on differences between the destination sequence numbers of the received RREPs.

In [12], Disha et al have proposed algorithm based on course based scheme. In this scheme node does not observe every nodes but only observes node in current route path. In this scheme every node should maintain packets digest buffer i.e. Fwdpacketbuffer. This algorithm is divides into three steps 1).when packet is forwarded, its digest is added in Fwdpacketbuffer and detecting node overhear. 2) When next node forward packet is overhead, the digest will freed from Fwdpacketbuffer. 3) In fixed period of time, detecting node should calculate overhear rate of its next hop and compare it with a threshold. Then we measure overall throughput to analyze how gray hole attack effects the network performance under different no. of attacks as well as different gray magnitude.

VI. CONCLUSION

Mobile Ad-hoc networks are seen as a key in the evolution of wireless networks. Security is the most important feature for deployment in MANET. In this paper we have seen the how black hole and gray hole attack happened in network layer .Due to its dynamic nature, MANET prone to different limitations and weakness. Our aim is to detect and mitigate the false node which is acting as a normal node, which is very hard to find out. But if we design a new approach of detecting the attacker node we can ensure that there is a safety in the network. Once security is lost in the network then the entire network will get failed. The main goal of this paper is to detect and prevent gray hole attack and black hole attack then we should be improve the security and as well as the performance of the network. During the survey we addressed how the attack has been happened in the network layer.

VII. REFERENCES

[1] Amitabh Mishra and Ketan M. Nadkarni, "Security in Wireless Ad Hoc Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[2] Banerjee, s., "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks", in proceedings of the world congress on engineering and computer science, 2008.

[3] Jain, S., Jain, M., and kandwal h., "Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks", J. Computer applications, vol. 1, no. 7, 37-42, 2010.

[4] N. H. Mistry, D. C. Jinwala and M. A. Zaveri, "MOSAODV: Solution to Secure AODV against Black hole Attack", (IJCNS) International Journal of Computer and Network Security, Vol. 1, No. 3, December 2009.

[5] Mr. L Raja 1, Capt. Dr. S Santhosh Baboo," Comparative study of reactive routing protocol (AODV, DSR, ABR and TORA) in MANET", International Journal of Engineering and Computer Science, ISSN: 2319-7242 Volume 2 Issue 3 Page No. 707-718, March 2013.

[6] J. Luo, M. Fan, D. Ye, "Black hole attack prevention based on authentication mechanism," 11th IEEE Singapore International Conference on Communication Systems, 2008. ICCS 2008. pp. 173-177, Guangzhou, 19-21 Nov. 2008.

[7] Rajesh Yerneni, Anil K. Sarje, "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks", IEEE conference on ICCCNT' 12, Coimbatore, India 26th- 28th July , 2012.

[8] H.Deng; W.Li; D.Agarwal, "Routing security in wireless ad hoc networks",[J]. Communication Magazine, IEEE, (2002), 70-75.

[9]. Chen Wei Long, Xiang Bai Yuebin, Gao Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", IEEE conference on Communications and Networking in China, 2007. CHINACOM '07, pp. 366 – 370, 22-24 Aug. 2007.

[10] K. Lakshmi, S.Manju Priya, A.Jeevarathinam K.Rama, K.Thilagam, "Modified AODV Protocol against Blackhole Attacks in MANET", Karpagam University, Coimbatore. International Journal of Engineering and Technology Vol.2 (6), 2010.

[11] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007, PP:338-346.

[12] Disha G.Karriya, Atul B. Kathole, Sapna R.Heda, "Detecting black and gray hole attacks in mobile ad hoc network using an Adaptive method", IJTAE, 2012.