REVIEW OF DIFFERENT TECHNIQUES USED FOR DETECTION AND APPEASE BLACK HOLE ATTACK IN AODV ROUTING PROTOCOL

Vishal Vig[1], Rishi Sharma[2]
[1,2]Department of Computer Science & Engineering
Quantum School of Technology, Roorkee, Uttarakhand

Abstract

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. Hence, a MANET can be constructed quickly at a low cost, as it doesn't rely on existing network infrastructure. This paper presents a review on different techniques used to detect and mitigate the black hole attack in MANET i.e. for single black hole and also for cooperative black hole attack which are a serious threat to ad hoc network security. In cooperative black hole attack multiple nodes collude to hide the malicious activity of other nodes; hence such attacks are more difficult to detect. In this paper a comparison of various techniques that have been proposed in the literature for detection and mitigation of such attacks is presented.

Keywords: Mobile Ad Hoc network, Single Black hole attack, Cooperative Black hole Attack, AODV Routing Protocol

1. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are wireless multi-hop networks dynamically constructed by autonomous mobile nodes without the support of any infrastructure or centralized administration. Nodes communicate directly if they are within each other radio range via wireless links, while those which are far apart relay their messages through other nodes.

This new paradigm of wireless communications aims to make communication possible in some situations where the services offered by both wired networks and WLAN are unavailable. MANETs are mainly useful in situations where no fixed infrastructure is available, such as, military applications, natural disasters, and rescue missions.

MANETs are prone to various types of active and passive attacks. Active attacks are categorized into Interception, interruption, fabrication and modification attacks. A passive attacker does not interrupt with the operation of a routing protocol but puts efforts to gather the vital information from packets. MANET has proactive, reactive and hybrid routing protocols.

In proactive protocols the routes to all parts of the network or the destinations is determined at the starting time and a route update table is maintained periodically In reactive protocols the route discovery process is carried out for establishing the routes as and when required. Mostly used protocols are Ad-hoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Hybrid protocols employ a hierarchical strategy these protocols adhere to combination of properties of both proactive and reactive protocol.

A. Black hole Attack in MANET

This is the most frequent attack that happens when packet are forwarded. The attacker uses routing protocol to advertise itself as having a authenticate route to a destination node. An attacker uses the flooding based protocol for listing the request for a route from the source. Then attacker creates a reply message having shortest path to the destination. As the result, the attacker

reached to the source before the reply from the actual node and then source assume that it is the shortest path to the destination.
Therefore a fake route is created. Once the attacker has been able to introduce himself between the communications nodes, then attacker may free to do anything with the packet which is send by source for the destination

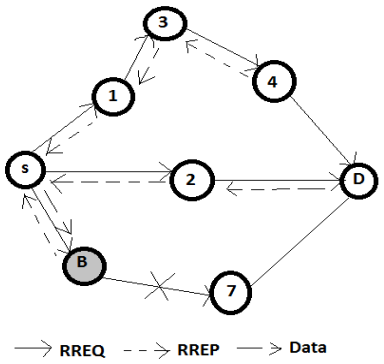

Figure 1 Black Hole Attack in MANET
In figure 1. Node 'B' is acting as a malicious node. When node 'S' wants to send some data to node 'D', it broadcast RREQ packet in network. Node '1', '2' & 'B' receives it. Node 'B' being a malicious node do no check in its routing table for route and unicast RREP packet to source. Node 'S' receive reply from node 'B' ahead of other nodes & consider it as shortest path and start sending data to 'B' Malicious node instead of forwarding data packets, drop them and thus hider the network performance.

2. LITERATURE REVIEW

[1] Jain & Khuteta 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. Only malicious node will send a reply as they do not check in their table for route to destination. Base Node lists all the nodes that have sent reply and generate a block message which is to be broadcasted to all nodes in the network. After receiving the block message, the other nodes add identity of black hole node in their block table and isolate it from further communication.
With the proposed solution, the performance of PDR, end-to-end delay and throughput are improved in the presence of malicious node.

[2] Chaube et al. 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 Black 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 black hole attack TSDRP demonstrate better performance in almost all parameters: PDF, AED, AT and NRL as compared to AODV.

[3] Gupta & Rana surveyed regarding the various kind of attacks happened on the network layer in MANET. The survey is regarding the various kinds of attacks happened in the network layer in MANET and measures the performance of AODV with DOS, Black Hole and Gray Hole attack. Performance is based on the basis of matrices like throughput, END to END delay and packet loss. 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.

[4] Gupta proposed a new method RTMAODV (Real Time Monitoring AODV). It does not introduce any overhead. Moreover neighbour node detects and prevents black 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 neighbour node of Route Reply (RREP)

sender node i.e. suspected node. Two counters as fvalue and rvalue are used for performing a check on malicious node. These are used for counting number of forwarded packets and number of received packets respectively. fvalue reaches a threshold value and rvalue is 0 then node is considered to be malicious and is discarded from the network by broadcasting INTNOT Packet. In simulation, new method has shown outstanding result in terms of packet delivery ratio as compare to AODV routing protocol in presence of malicious node under black hole attack.

[5] Arya et al. instigate to detect and avoid the wormhole attack and collaborative black 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 neighbouring node and second its relationship status with the neighbour node that could be Most Reliable, Reliable or Unreliable. Initially when node joins the networks they are considered as an Unreliable. The Throughput, energy of Wormhole Attack and Collaborative Black hole attack of AODV is more as compare to Trusted AODV, when they increase the time, there is little bit effect in throughput, energy level of both is decreased. Packet delivery ratio is also better in case of Trusted AODV.

[6] Ranjan et al. have focused on the black hole attacks. These black 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. In such kind of attacks a node advertise a shortest path for the given route request and redirects the data path through itself getting an easy access to all the data being transferred. Such nodes are called as malicious nodes. 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 black hole attacks.

[7] Hiremani & Jadhao planned to detect and eliminate co- operative black hole and gray hole attacks by maintaining MEDRI (Modified Extended Data Routing Information) Table at each node. The fields of this table are used to detect a malicious node as well as maintain a history of its previous malicious instances toaccommodate the
Gray hole behaviour. The MEDRI table also record and maintain the history of the previous malicious nodes that is used for the future secure transformation of data from source to destination and to discover secure path from source to destination.

[8] Tan & Kim Proposed a solution in which it has defined different threshold value for different environment like small medium and large. The threshold value defined is some percentage of the maximum destination sequence number. In this two extra functions are added i.e. Source node use threshold value to verify RREP from neighbor nodes and destination Node use the defined threshold to verify the RREQ messages from source node. If the destination sequence number of RREP is greater than threshold it is considered as malicious node. Destination node also uses threshold value to identify the destination sequence number.

[9] Wahane & Lonare proposed an Algorithm to detectcooperative Black hole Attack and examination has been done by considering three different cases. In the first case there was no malicious node present in the network. In the second case there were two black hole nodes in the network Mutually cooperating with each other. In the third case a node is found to be reliable and this information is broadcasted throughout the network and third bit with respect to that node is set to true which shows that the node in question is trustful node. Finally it has been concluded that this algorithm works well in all the three cases with the aim of detecting Cooperating Black hole Attack

and ensuring a secure as well as reliable route from source to destination.

[10] Kshirsagar & Patil proposed a solution, this method first identifies the neighbor of the RREP node creator i.e. suspected node. Neighbor node is instructed to listens the packets send by suspected node. fcount and rcount are the two counters maintained by neighbor node. When a neighbor node forwards any packet to suspected node it will increase the fcount counter by 1. If suspected node forward a packet it will be overheard by the neighbor node and rcount is increased by 1. After source node receives RREP it sends packets to path to check the node is malicious node or not. Neighbor node forwards packets to suspect node until fcount reaches a threshold; thereafter if rcount is 0. RREP creator will identify as malicious node and blocked.

Table 1: A Survey on Different Proposed Methods to detect and mitigate the attacks in the network:

S. No.	Research Paper	Year	Method	Black hole Nodes	Network Parameters	Future Scope
1.	Black hole Attack Detection And prevention by real time monitoring	2015	Real Time monitoring of Nodes	Detect Single Black hole Node	Increase in PDR and End-to-End Delay	Detect a cooperative Black hole node attack using real time monitoring
2.	Detecting Warm hole attack and Black hole attack in MANET	2015	Trusted AODV	Detect Cooperative Black hole Node	More PDR, More Throughput and Less Energy	Calculate Trust value for other attacks in MANET
3.	Performance analysis of TSDRP and AODV under Black hole Attack	2015	TSDRP	Detect Single Black hole Node	Better Performance in PDF, AED, AT and NRL	Performance metrics of other parameters can be calculated
4.	Detecting and Overcoming Black hole Attack in MANET	2015	Malicious Node is detected by deploying	Detect Single Black hole Node	Increase in PDR, End-to-End Delay and Throughput	More than one Base Nodes can be deployed in the Network
5.	Assessment of Various Attacks on AODV in Malicious Environment	2015	Highest Sequence Number of the Nodes	Detect Single Black hole Node	Throughput and End-to-End Delay decreases as SimulationTime increases	

6.	Secure Route Discovery for preventing Black hole Attacks in MANET	2013	SRD - AODV	Detect Single Black hole Node	Increase in PDR, routing overhead increased in comparing the sequence number with threshold value	Security mechanism for data transmissions between the source node and destination node after a route has been established
7.	Secure AODV to Combat Black Hole Attack in MANET	2013	Modified RREP	Detect Single Black hole Node	Better Security Mechanism to AODV	
8.	Eliminating Cooperative Black hole and Gray hole Attacks in MANET	2013	Modified EDRI Table	Detect Cooperative Black hole Nodes	Maintains the history of previous Black hole nodes in the network	

3. CONCLUSION

In this paper we have discussed the methods for detection and prevention of black hole attack in MANET. Black hole Attack in Manet is a Denial of Service Attack which reduces the network performance. The study here shows different methods of AODV protocol which have been proposed and implemented to prevent and detect Black hole attack. A comparison table shows the performance of methods and their Future work for Single Black hole and also for Cooperative Black hole Attacks.

REFERENCES

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

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

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

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

[6] Rakesh Ranjan, Nirnemesh Kumar Singh, Ajay Singh "Security Issues of Black Hole Attacks in MANET"International Conference on Computing, Communication and

Automation (ICCCA 2015).
[7]Vani A. Hiremani,ManishaMadhukar Jadhao, “Eliminating Co-operative Black hole and Gray hole Attacks Using Modified EDRI Table in MANET” IEEE 2013.
[8] Seryvuth Tan, Keecheon Kim, “Secure Route Discovery for Preventing Black 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.
[9] Gayatri Wahane, Savita Lonare, “Technique for Detection of Cooperative Black Hole Attack in MANET” 4th IC CCNT 2013, Tiruchengode, India.
[10] Durgesh Kshirsagar, Ashwini Patil, “Black hole Attack Detection and Prevention by Real Time Monitoring” IEEE 2013.