ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 5, May 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Review Paper on Black Hole Attack in MANET

Aanchal Joshi
M.tech., Department of Computer Science
Seth Jai Prakash Mukand Lal Institute of Engineering And Technology(JMIT)
Kurukshetra University – India

Abstract: ***Ad-hoc networks have become a new standard of wireless communication in infrastructure less environment. MANET is a Mobile Ad-hoc Network which is a collection of multi-hop wireless mobile nodes that communicate with each other without centralized control. The primary challenge for building a MANET is equipping each device to continuously maintain the data required to properly route traffic.They are spontaneous in nature and absence of centralized system makes them susceptible to various attacks. Black hole attack is one such kinds attack in which a malicious node advertises itself as the best route to the destination node and hinders the normal services provided by the network. Ad hoc On-demand Distance Vector(AODV) and ZRP are the most suitable routing protocols for the MANETs and they are more vulnerable to black hole attack by the malicious nodes. A malicious node that incorrectly sends the RREP (route reply) that it has a latest route with minimum hop count to destination and then it drops all the receiving packets. This is called as black hole attack. This paper deals with the study aspect of this black hole attack.***

Keywords: Black hole attack, Mobile Ad-hoc Network, AODV, ZRP, Routing Protocols, Proactive, Reactive.

I. INTRODUCTION

The goal of Mobile ad hoc networks technology is to encourage internet access anytime and anywhere, without any pre-defined infrastructure and environment, which supports the mobility of the user, where network intelligence is placed into every mobile device.[1] Due to its self-maintenance and self configuration capabilities MANETs have several types of applications like search and rescue operations, sensor networks, military and security operation, conferencing, law enforcement and home network. MANET is an emerging area of research with practical applications.[2] However, MANET is especially vulnerable due to its fundamental characteristics, such as open medium, distributed cooperation, distributed cooperation, and constrained capability. Routing plays vital role in the security of the whole network. Thus operations in MANET introduce few new security issues in addition to the ones already present in fixed networks. Network attacks occurs when an intruder tries to exploit vulnerabilities of any system. There are many types of attacks in MANET.[4] Generally speaking, these attacks are classified into two broad categories: passive and active attacks. In passive attacks, the attackers typically involve eavesdropping of data, thus disclose the information of the location and move patterns of mobile nodes. This kind of attacks is very much difficult to find, because the attacker seldom exhibits abnormal activities. Active attacks, on the other hand, involve actions performed by intruder. The target of the attack can be either data traffic or routing traffic. The intruders may add large amount of extraneous data packets into networks. They can also intentionally drop, delay and corrupt data packets passing through it.

Routing in MANETs is classified as Reactive (Ondemand) Routing and Proactive (Table driven) Routing. A reactive protocol initiates routes whenever they are needed whereas proactive protocols maintain consistent and up-to-date tables which contain routing information from each node to every other node. Here, we are considering reactive routing protocol such as AODV. Since no security mechanism is provided by AODV, attack can be performed by any malicious node by disobeying the protocol specifications. The major AODV vulnerabilities are decrementing Deceptive incrementing of Sequence number and Hop Count.[3] Black hole attack is an attack in which all the packets in a network are redirected to a specific node that falsely

claims to have fresh route, and absorbs or drops those packets without forwarding them to other or destination nodes. This proposed technique gives a better solution towards Black Hole Attack within the network. The Black Hole attack with four different scenarios with respect to the performance parameters of Average Network Delay, Network Throughput, Total Dropped Packets and Packet Delivery Ratio has been simulated. We can see there is a boundary overlapping is major issue in ZRP protocol. Also, there is a need to analyze Black Hole attack in other MANETs routing protocols such as TORA, GRP and FSR. Also other types of attacks such as Wormhole, Jellyfish, Sybil, Byzantine attacks are needed to be studied in comparison with Black Hole attack. They can also be categorized on the basis of how much they affect the performance of the network.

II. ROUTING PROTOCOLS

Designing an efficient routing protocol in MANET's is very challenging problem. And also provide different level of Quality of Services to different types of application [2]. Routing protocols are used for communicating or broadcasting routing information to the target node. Routing protocols are classified in to three categories: proactive, reactive and hybrid.

A. Proactive Routing Protocol:

The proactive routing protocol is also known as Table-Driven Routing Protocol. In this, nodes are periodically transfers its routing information to its neighbour nodes which is come into its transmission range. It is maintain its routing table up to date. The main disadvantage of this routing protocol is that, it creates overhead in the network due to periodically transfers routing status. And the advantage is that, if any attacker node joined in network is finding immediately using routing table information. Destination Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OSLR) are most familiar types of routing protocols of proactive routing protocol.

B. Reactive Routing Protocol:

The reactive routing protocol is also known as On-Demand Routing Protocol. In this, as name suggest, the routing information is transferred when it is required. It creates lower overhead than proactive routing protocol. This routing protocol is also affected from the malicious node. Disadvantage is that leads to some packet loss. Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR) is most familiar routing protocols of active routing protocol.

C. Hybrid Routing Protocol:

The hybrid routing protocol is invented using the advantages of reactive and proactive routing protocols. It is related to Hierarchical Network Architecture. It uses the advantage of proactive routing protocol is that, get complete information of route and uses advantage of reactive routing protocol is that, when network topology changed it maintain its routing table. Zone Routing Protocol (ZRP)[12], Temporally-Ordered Routing Algorithm (TORA) is most familiar kinds of routing protocol of hybrid routing protocol.

- **Zone Routing Protocol(ZRP)**

The Zone Routing Protocol [10], as its name implies, is based on the concept of zones. A routing zone is defined for each seperate nodes, and the zones of neighboring nodes overlap. The routing zone has a radius r expressed in hops. The zone will include the nodes, whose distance from the node in question is at most r hops. An example of routing zone is shown in Fig. 2, where the routing zone of S includes the nodes A–I, but not K. In the illustrations, the radius is marked as a circle around the node in question. It should be noted that the zone is defined in hops, not as a physical distance. The nodes of a zone are divided into peripheral nodes and interior nodes. Peripheral nodes are nodes whose minimum distance to the central node is exactly equal to the zone radius r. The nodes whose minimum distance is less than r are interior nodes.

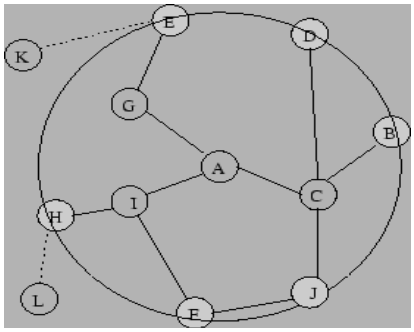

Fig.2 Zone Routing Protocol

- **Black hole Attack**

Black holes refers to places in the network where incoming or outgoing traffic is silently discarded (or dropped), without informing the source node that the data did not reach its intended recipient. Black holes are actually invisible and can only be detected by monitoring the lost traffic. In black hole attack, attackers embeds itself into the route from source though destination by sending a false RREP containing higher sequence number giving that Impression that it has the freshest route towards destination. Then the source will be captured into constructing a path through malicious nodes and rejecting all other available paths. After doing that, when the data packets are to be transmitted towards destination, the attacker will simply drops all of them and thus destination will not be able to receive even a simply piece of information.

Black hole Attacks are classified into two categories :

1. Single Black Hole Attack

In Single Black Hole Attack only one node acts as malicious node within a zone. It is also known as Black Hole Attack with single malicious node. Collaborative Black Hole Attack [10].In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

2. Collaborative Black Hole Attack

In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

Techniques of Blackhole Detection:

There is lot of work done in MANET for detection of Black Hole attacks some of existing techniques of it for different routing protocols are as follows:

TABLE 1: Techniques of Detecting Blackhole Detection

	Routing protocol	***Simulator***	***Results***	***Defects***
I. Neighborhood based And Routing Recovery	AODV	NS-2	The probability of one attacker can be detected is 93%	Failed when attackers cooperate to forge the fake reply packets
II. Random Two hop ACK and Bayesian Detection Scheme	DSR	GloMoSimbased	The true positive rate can achieve 100% when existing 2 witness	The proposed scheme is not efficient when k equals to 3, reducing the true positives
III. DPRAODV	AODV	NS-2	The PDR is improved by 80 85% than AODV	A little bit higher routing overhead and

			when under blackhole attack	end-to-end delay than AODV
IV. IDS based on ABM	MAODV	NS-2	The packet loss rate can be decreased to 11.28% and 14.76%	Cooperative isolation the malicious node, but failed at collaborative blackhole attacks
V. Prevention of Black Hole Attack in Mobile Ad-Hoc Network	AODV	NS-2	Provides better Additional Security	Decreased PDR and end to end Delay
VI. Bluff-Probe Based Black Hole Node Detection and prevention	ZRP	Qualnet	Provides low overhead and better performance	Used only for light weight network
VII. Enhancing Security of Zone-Based Routing Protocol using Trust	ZRP	NS-2	Improves packet Delivery Ratio	Cost of this improvement increased in end to end and routing overhead

III. Related Work

Ayesha Siddiqua et al. in proposed mobile ad hoc networks (MANETs) which are the collection of mobile hosts which communicate with each other with no central network authority or fixed infrastructure. Due to its characteristics like mobility and heterogeneity ad hoc networks are more vulnerable to attacks. Black hole is an attack where all the packets forwarded to attacker node, by neighboring nodes, are dropped intentionally. In this paper, we propose a secure algorithm which aims to detect and prevent the black hole by considering the packet drop reasons in promiscuous mode. Existing AODV routing protocol is modified to detect and prevent the black hole attack. The experiment results show that our proposed algorithm secure the AODV against black hole attack in MANETs.[1]

S.Sankara Narayanan and Dr.S.Radhakrishnan et al, proposed a defense mechanism against a coordinated attack by multiple black hole nodes in a MANET. The simulation carried out on the proposed scheme has produced results that demonstrate the effectiveness of the mechanism in detection of the attack while maintaining a reasonable level of throughput in the network.

Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan et al [7] Mobile Ad hoc Network (MANET) is a group of wireless nodes that are distributed without relying on any standing network infrastructure. MANET routing protocols were designed to accommodate the properties of a self organized environment without protection against any inside or outside network attacks. a Local Intrusion Detection (LID) security routing mechanism to detect Black Hole Attack (BHA) over Ad hoc On Demand Distance Vector (AODV) MANET routing protocol. In LID security routing mechanism, the intrusion detection is performed locally using the previous node of the attacker node instead of performing the intrusion detection via the source node as in Source Intrusion Detection (SID) security routing mechanism. By performing LID security routing mechanism, the security mechanism overhead would bedecreased. Simulation results using the GloMoSim simulator show that the improvement ratio of the throughput gained by LID security routing mechanism and overall improvement reduction in the end-to-end delay and routing overhead.

IV. PROPOSED SOLUTION FOR BLACK HOLE

- **First Solution**

In this solution, the sender node will needs to verify the authenticity of the node that initiates the RREP packet by utilizing the network redundancy. Since any packet can be arrived to the destination through many redundant paths, the idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time period, the sender node will buffer its packets until a safe route is identified. Once a safe route has identified, these buffered packets will be transmitted. When a RREP arrives to the source, It will extract the full paths to the destinations and wait for another RREP. Two or more of these nodes must have some shared hops (in ad hoc networks, the redundant paths in most of the time have some shared hops or nodes). From these shared hops the source node can recognize the safe route to the destination. If no shared nodes appear to be in these redundant routes, the sender will wait for another RREP until a route with shared nodes identified or routing timer expired. This solution can guarantee to find a safe route to the destination, but the main disadvantage is the time delay. In addition, if there are no shared nodes or hops between the routes, the packets will never been sent.[9]

- **Second Solution**

Every packet in MANETs has a unique sequence number. This number is an increasing value, i.e., the next packet must have higher value that of current packet sequence number. The node in regular routing protocols keeps the last packet sequence number that it has received and uses it to check if the received packet was received before from the same originating source or not. In this solution, every node needs to have two additional small-sized tables; one to keep last-packet-sequence-numbers for the last packet sent to every node and the other to keep last packetsequence-numbers for the last packet received from every node. These tables are updated when any packet arrived or transmitted. The sender broadcasts the RREQ packet to its neighbors. Once this RREQ reach the destination, it will initiate a RREP to the source, and this RREP will contain the last packetsequence- numbers received from this source. When an intermediate node has a route to the destination and receives this RREQ, it will reply to the sender with a RREP contains the last packet- sequence numbers received from the source by this intermediate node. This solution provides a fast and reliable way to identify the suspicious reply. No overhead will be added to the channel because the sequence number itself is included in every packet in the base protocol.

- **Third solution**

The algorithm for Modified-Zone Routing Protocol is as follows:

Step 1. Find neighbor node along with a source node of the protocol.

Step 2. Source node will check routing table entries for these particular neighboring nodes in the protocol.

Step 3. Choose a neighbor node as a reliable node and get IP address of selected reliable node.

Step 4. Now to detect Black Hole node it will send request to outlying nodes.

RREQ (sndr_t dst) for reliable node's IP.

Step 5. Get reply for request from the outlying nodes RREP(sndr_t ipdst).

Step 6. Check intermediate nodes which replied along with source's routing table.

Step 7. If any intermediate node is present as outlying node in source's routing table then mark that node which replied as Black Hole node and broadcast alarm packet message about that node and alert the other nodes to update their routing tables so as to prevent Black Hole attack.

V. CONCLUSION

Due to the inherent design drawbacks of routing protocol in MANETs, many researchers have conducted diverse techniques and solutions to propose different types of prevention mechanisms for black hole attack problem.

According to this work, we observe that both of proactive routing and reactive routing have specialized skills. The proactive detection method has the better packet delivery ratio and correct detection probability, but suffered from the higher routing overhead due to the periodically broadcast packets. The reactive detection method eliminates the routing overhead problem from the event-driven way, but suffered from some packet loss in the beginning of routing procedure. Therefore, we proposed a hybrid detection method (ZRP)which combined the advantages of proactive routing with reactive routing is the tendency to future research direction. This proposed technique gives a better solution towards Black Hole Attack within the network. The Black Hole attack with four different scenarios with respect to the performance parameters of Average Network Delay, Network Throughput, Total Dropped Packets and Packet Delivery Ratio has been simulated. We can see there is a boundary overlapping is major issue in ZRP protocol. Also, there is a need to analyze Black Hole attack in other MANETs routing protocols such as TORA, GRP and FSR. Also other types of attacks such as Wormhole, Jellyfish, Sybil, Byzantine attacks are needed to be studied in comparison with Black Hole attack. They can also be categorized on the basis of how much they affect the performance of the network. The black hole problem is still an active research area.

References

1. Ayesha siddiqua,kotari sridevi,Arshad Ahmad khan Mohammed''preventing Black hole Attacks in MANETS using secure Knowledge Algorithm"SPACES-2015,Dept of ECE,KL UNIVERSITY.
2. Radhika K. Vyas''Blackhole Attack Detection/Prevention Techniques in MANET'' Volume-2, Issue-5, May-2015.
3. Dr.A.A Gurjar,A.A Dande"Black hole attack in MANETS"International Journal of IT,Engineering and Applied sciences Research(IJIEASR)Volume2,No.3,March 2013.
4. Barleen Shinh,Manwinder Singh"A Review paper on collaborative Black hole Attack in MANETS"International journal of Engineering and computer science ISSN:2319-7242 Volume 3 Issue 12 december 2014,page No. 9547-9551.
5. Kishor Jyoti Sharma,Rupam Sharma,Rajdeep Das"A Survey of Black hole Attack Detection in MANET" 978-1-4799-2900-9/14/$31.00 ©2014 IEEE
6. F.Stajano and R.Anderson,"The Resurrecting Duckling:Security Issuesfor Ad-hoc wireless Network",Security protocols,7th International workshop proceeding,lecture,Notes in computer science university of Cambridge computer laboratory.
7. Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan"A Local Intrusion Detection Routing Security over MANET Network" International Conference on Electrical Engineering and Informatics, Bandung, Indonesia.
8. Fan-hsun,Li-Der Chou and Han-chieh chao"A survey of black hole attacks in wireless mobile ad-hoc networks"Tseng et al. Human-centric computing and Information science.
9. Mr.Alok Sharma" The Black-hole node attack in MANET" 2012 Second International Conference on Advanced Computing & Communication Technologies.
10. Chaitas Shah"Improving ZRP Protocol against Blackhole Attack"2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939
11. S.Sankara Naryanan and Dr.S.Radhakrishnan"secure AODV to combat Black hole Attack in MANET"2013 International conference on Recent trends in Information Technology (ICRTIT).
12. kriti gupta"Secure Detection Technique Against Blackhole Attack For Zone Routing Protocol in MANETS" Volume 2, Issue 6, June 2013.

