International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

A study of various Black Hole Attack techniques and IDS in MANET

Ajesha Patel
Department of Computer Science and Engineering
Radharaman Institute of Technology and Science
Madhya Pradesh, Bhopal, India

Anurag Jain
Department of Computer Science and Engineering
Radharaman Institute of Technology and Science
Madhya Pradesh, Bhopal, India

***Abstract* -Mobile Ad Hoc Network (MANET) is said to be as a group of wireless mobile nodes vigorously forming a impermanent network that does not use any accessible heterogeneous network infrastructure. In this period of wireless devices, Mobile Ad-hoc Network (MANET) has become an inseparable element for communication for mobile device. Consequently, significance in research of Mobile Ad-hoc Network has been growing since last few years. Due to this it is vulnerable to various kinds of security threats. Black hole attack is one of such threats. This paper lead emphasis on the detection and prevention of the malicious nodes (black hole)by using AODV protocol in order to secure the overall network. AODV is an on-demand routing protocol that tries to discover a path only at the time when there is a requirement from mobile nodes in the network.**

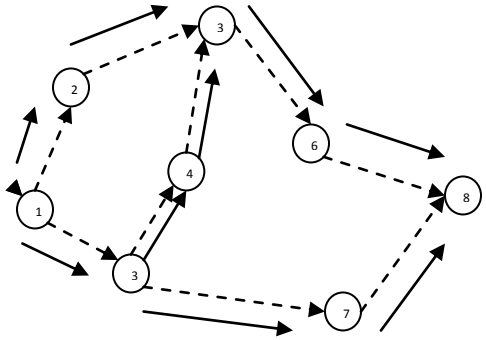
Keywords: Black hole Attack; AODV; MANET; Security Threats; Route discovery

I. INTRODUCTION

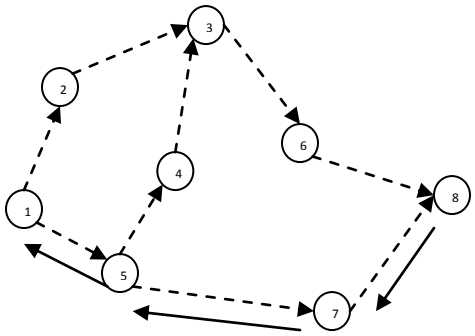
Mobile ad-hoc networks are composed of independent nodes that are self- managed lacking any layout. Ad-Hoc networks are composed of dynamic topologies in which nodes can readily enter or leave the network arbitrarily. Thus this network is appropriate for areas where it is unfeasible to set up a fixed Infrastructure. In MANET, nodes offer links by using different routing protocols and AODV is one of the extensively used routing protocols in mobile Ad-hoc network.

In AODV the source node requires to send a message to some receiver node and it did not have a applicable route to the receiver, the source node initiates a path finding process for allocating all other node in the network. It then broadcasts a route request (RREQ) packet to the nodes in its close proximity, later transmitted further to their nearby nodes. This process continues to the extent up to which the receiver or an intermediate node with a "fresh" path to the target is located. When the RREQ message packet either reaches the destination node or encounters a node with a route to the destination a response is entrusted. That response occurs via the transmission of a route reply (RREP) message. In case if a node realizes that the route is damaged or broken it transmits a route error (RERR) message to the source.

Route discovery is a susceptibility of on-demand routing protocols, more specifically AODV, it can be exploited by an opponent to execute a black-hole attack on mobile ad-hoc networks. A pernicious hub in the system accepting a RREQ message answers to destination hub) to source hubs that it malevolent hub on the grounds that entire hubs in sending a fake RREP message that contains alluring parameters to be picked for parcel conveyance to destination hubs. data contains in the RREP message source hubs (by to affirm it has a way to forward information, a malevolent hub starts to disturb and drop all the network traffic that is received from source nodes and make it slow. This intentional dropping of packets by a malicious node is what we call a black hole attack.



(a) Propagation of Route Request(RREQ) packet [1]



(b) Path taken by the Route Reply(RREP) packet[1]

Source: NODE 1
Destination: NODE 8

II. RELATED WORK

Sanjay Ramaswamy et al worked on Prevention of Black Hole Attack. In this paper, they have address the difficulty of synchronized attack by numerous black holes acting in assembly .They present a technique to recognize multiple black holes attacks working with each other and a way out to determine a safe path avoiding mutual black hole attack. They anticipated a methodology for identifying multiple black hole nodes cooperating as a group with slightly customized AODV protocol by introducing a table called Data Routing Information Table (DRI) and Cross Checking. [5]

Fan-Hsun Tseng et al, in this paper, they have done a survey on the available solutions and discuss the routing methods. They not only grouped these proposals into two group i.e. single black hole attacks and collaborative black hole attacks but also scrutinize the categories of these solutions and give a comparison table. In this the routing protocol like table driven are used in which mobile nodes occasionally broadcast their routing information to the neighbors. [6]

AODV directing capacities utilizing 2 stages; course disclosure and course support. Amid course disclosure the hub will surge the system with course asks for (RREQ) utilizing an extended ring pursuit instrument which works in a comparative way as the time-to-live (TTL) in customary wired systems. This highlight constrains the span of the system surge to decrease data transfer capacity use; ought to a course not be discovered the solicitation will be telecast again with a bigger TTL esteem. [15]

At the point when a destination hub gets a RREQ parcel it will utilize the separation vector steering to build an opposite way and send a unicast course answer bundle (RREP) to the source, this bundle will return along the course it ventured out to achieve the destination [16], every hub it goes through keeps up a provisional course store for the term of the correspondence.

Ei Ei Khin1 and Thandar Phyu2 worked on the impact of black hole attack on On-Demand Distance Vector (AODV) protocol. For the recreation, IEEE 802.11 Mac at the physical and data link layer is applied. The channel is a Wireless Channel works on Two Ray Ground radio propagation model. AODV is applied at the network layer as on dissimilar system execution measurements, example, parcel conveyance degree, standardized steering overhead normal end to end delay, bundle conveyance The AODV directing convention is one that is utilized at the system layer as the directing convention and UDP is utilized at the vehicle layer the routing protocol and UDP is applied at the transport layer. [7]

Saurabh Gupta et al studied Black hole Attack Avoidance Protocol for Wireless Network, a protocol that is used for avoiding black hole attack lacking the restraint of special hardware and dependence on physical medium of wireless network. BAAP forms relation disjoint multi-path throughout the path detection to give better path choice in order to avoid malicious nodes in the course using authenticity table maintained by each node in the network. Non-malicious nodes progressively isolate the black hole nodes based on the values composed in their authenticity table and avoid them while constructing path between source and destination. [8]

.Bhoomika Patel and Khushboo Trivedi worked on Prevention and Detection of Black Hole Attack in AODV based on MANET. In this paper, they have focused on AODV Routing protocol which is Reactive protocol. They have studied and contrasted the current arrangements with dark gap assaults on AODV convention. This paper attempts to detect and divide malevolent nodes, selectively tries to execute black hole attacks by deploying IDSs in MANETs. [9]

Aikaterini Mitrokotsa and Christos Dimitrakakis In this paper some strategies are applied in interruption location for MANETs. With a precise end goal to do as such they evaluate five administered order calculations for interruption location on various dimensions. They measure their implementation on a dataset, explained in this paper, which incorporates differed activity conditions and paper. [10]

Meenakshi Tripathi,M.S.Gaur,V.Laxmi compared the Impact of Gray Hole and Black Hole Attack on LEACH. The paper gives a summary of LEACH, the most accepted clustering routing protocol in WSN. The routine of WSN under attack is carefully investigated, by applying it on different network parameters with a variety of node densities. It is observed that the effect of the Black Hole attack is further on the network performance as compared to the Gray Hole attack. [11]

Ming-Yang Su, in this paper, several IDS nodes are deployed in MANETs with a specific end goal to distinguish and counteract particular dark gap assaults. The IDS hubs must be set in sniff mode with a specific end goal to perform the purported ABM (Anti-Black hole Mechanism) the proposed IDS can perform exceptionally well When a suspicious worth surpasses a limit, an IDS adjacent will show a square message, educating all hubs on the system, asking them to helpfully segregate the pernicious hub. This study utilizes ns2 to as IDS hubs can quickly hinder a vindictive hub, without false positives, if a fitting limit is situated. [12]

Na Li, Sajal K. Das In this paper, they have intended a trust-based framework to more accurately estimate an encounter's delivery competency, which can be flexibly

integrated with a large family of existing data forwarding protocols designed for Opp Nets. As a case study, they integrate the proposed framework with PROPHET, and exhibit its effectiveness against ‘‘black hole’’ attacks through experimental study. [13]

Satoshi Kurosawa et al worked on Detecting Black hole Attack on AODV-based MANET, Dynamic Learning Method is applied for this purpose. In this paper, they proposed an abnormality detection scheme via dynamic training method here the training data is restructured at regular time intervals. The simulation results demonstrate the effectiveness of the scheme compared with conservative scheme. [14]

Rutvij, Sankita and Devesh proposed an answer for confining malevolent hubs [17]. The structures of RREQ and RREP can be adjusted and include a handle in the directing table alongside the current fields. I.e. a Malicious node list is added to the RREQ bundle field to tell different hubs about pernicious hubs in the adhoc system. Also, we add a banner called Do not consider to RREP to stamp/recognize answer from a pernicious hub [18]. In AODV, steering table fields are destination IP location, grouping number, bounce check, next jump IP address, antecedent rundown, time when passage terminates.

Ngai et al. [19] firstly has recommended a strategy for recognition of sinkhole assaults which incorporates the BS in the location procedure, bringing about a hoisted correspondence cost for the convention. The system is overflowed by the BS with a solicitation message including the IDs of the affected hubs. The influenced hubs answer to the BS with a message containing their IDs, ID of the following jump and the related expense. The data is then utilized from the BS to develop a system stream chart for recognizing the sinkhole. Other existing conventions assemble identifying systems for sinkhole assaults in sensor organizes that are in light of steering conventions normally sent in Ad-Hoc systems, similar to the Ad Hoc On-interest Distance Vector Protocol (AODV) [20] and the Dynamic Source Routing (DSR) Protocol. [21]

III. PROBLEM STATEMENT

After going through various research papers on black hole the major problems they came across were:-the vulnerability of the links, The intermittent nature of connectivity, The limited physical protection of each of the nodes, The absence of a certification authority, due to this the network performance degrades which leads to low network efficiency and low throughput.

IV. METHODOLGY

The basic methodology for preventing a network from a black hole attack is to first detect the malicious nodes in the network then in the next step to blacklist that node ,by performing these two steps the network can be prevented from the black hole attack hence increasing the performance.

- *PROTOCOLS*

Table Driven Routing Protocols

In these kinds of routing protocols every node maintains single or additional routing table which includes routing information of all the other nodes in the network. All hubs continue redesigning these tables to keep up most recent perspective of the system. Some accepted proactive protocols are DSDV, WRP etc. [2]

On Demand Routing Protocols

In this routing protocols, the hubs don't keep up any directing table nut they have a course store Routes are find powerfully just when a hub need to correspond with another hub with the assistance of the course disclosure method which is started by the source node. Some reactive routing protocols are DSR, AODV etc. [3]

Hybrid Routing Protocols

This kind of conventions consolidates the best highlights of table driven and on interest directing conventions. If there should be an occurrence of the intra-area directing, these conventions utilizes the table driven methodology, while in the event of between space steering these conventions utilizes the on them.

Parameters:

- *Throughput.*

Network throughput is the rate of successful message delivery over a communication channel.

Throughput = packet_sent/total_data

with total_data = packet_sent+packet_lost

- *Packet Delivery ratio.*

The proportion of parcels that are effectively conveyed to a destination contrasted with the quantity of bundles that have been conveyed by the sender.

Packet Delay Ratio = ∑ Number of packet receive / ∑ Number of packet send

- Packet Loss

The total number of packets dropped during the simulation.

Packet lost = Number of packet send – Number of packet received.

- *Efficiency*

The ratio of the useful work performed in a process to the total energy expended.

- Network load

The total traffic of packets on the network.

- *End to End delay*

End to end deferral time incorporate all the postponement taken by switch to search for the way in system utilization, engendering deferral, handling defer and End to end delay for bundle p .[4]
End to end delay np=start time np-end time np

- *ATTACKS*

PASSIVE ATTACKS
Passive Attacks try not to plan to disturb the operation of the specific system ,it means they do tend to modify the packets.
Different types of passive attacks are as follows:

1. Traffic Monitoring
2. Eavesdropping
3. Traffic Analysis
4. Syn flooding [1]

ACTIVE ATTACKS
Active Attacks causes editing of information stream or formation of false stream. They have the capacity to modify the ordinary system operation .Following are the various types of active attacks:

1. Wormhole attack
2. Black hole attack
3. Rushing attack
4. Location disclosure attack
5. Flooding
6. Sinkhole attack
7. Spoofing attack
8. Replay attack

VI. EXPECTED OUTCOMES

In this paper after studying different research paper in the field of detection and prevention of single black hole attack and cooperative black hole attack, found that there are some of the scheme is able to detect the black hole node in the network but they also have some restrictions like increases overhead and false positive or negative rate. So in my work, proposing a method which can efficiently minimize the overhead as well as resourcefully can detect the cooperative black hole node present in the network.

VI. CONCLUSION

Wireless ad hoc network has dynamic topology and self configuring network, due to these attributes it is more open to security attacks black hole attack is one of them. In this presents the literature for the prevention of black hole attack and analyze that the methods are able to detect the black hole node and intensify the throughput of the network but they increases the overhead and false positive and negative alarm rate. In future work, develop an algorithm which can efficiently minimize the all these shortcoming during the detection of black hole node.

REFERENCES

[1] "Performance Evaluation of AODV routing Protocol under Black Hole attack with varying Black hole nodes" , 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science.
[2] T. Lin, S. Midkiff, and J. Park, "A framework for wireless ad hoc routing protocols" , in WCNC (Wireless Communications and Networking). IEEE Computer Society, 2003, pp. 1162.1167.
[3] Arun Kumar, lokantha Reddy and Prakash Hiremath, "Performance comparison of Wireless Mobile Ad-Hoc Network Routing Protocols", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008.
[4] Sanjay Ramaswamy ,et al" Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105.
[5] Fan-Hsun Tseng1,et al" A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences 2011.
[6] Ei Ei Khin1," IMPACT OF BLACK HOLE ATTACK ON AODV ROUTING PROTOCOL", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.
[7] Saurabh Gupta et al" BAAP: Black hole Attack Avoidance Protocol for Wireless Network", International Conference on Computer & Communication Technology (ICCCT)-2011.
[8] Bhoomika Patel et al **"**A Review - Prevention and Detection of BlackHole Attack in AODV based on MANET", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2816-2818.
[9] Aikaterini Mitrokotsa et al," Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", Security and Cryptography Laboratory (LASEC), School of Computer and Communication Sciences, EPFL, Station 14, CH-1015 Lausanne, Switzerland.
[10] Meenakshi Tripathi et al," Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN", Malaviya National Institute of Technology, Jaipur, India.
[11] Ming-Yang Su ,"Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Department of Computer Science and Information Engineering, Ming Chuan University, 5 Teh Ming Road, Gwei Shan District, Taoyuan 333, Taiwan.
[12] Na Li ⇑,"A trust-based framework for data forwarding in opportunistic networks", CReWMaN Lab, Computer Science and Engineering Department, The University of Texas at Arlington, United States.
[13] Satoshi Kurosawa1 et al," Detecting Black hole 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.
[14] Zhang, M., and Chong, P.H.J. (2009). Performance Comparison of Flat and Cluster-Based Hierarchical Ad Hoc Routing with Entity and Group Mobility.WCNC 2009 proceedings of IEEE Communications Society.
[15] Liu, C., Chang, S. (2009).The study of effectiveness for ad-hoc wireless network. ICIS 2009, November 24-26, 2009 Seoul, Korea. pp.412-417.
[16] Rutvij H.Jhaveri1, Sankita J. Patel2 and Devesh C. Jinwala, "Novel Approach for Gray Hole and Black Hole Attacks in Mobile Ad-hoc Networks", 2012 Second International Conference on Advanced Computing & Communication Technologies.

[17] Rutvij H.Jhaveri1, Sankita J. Patel2 and Devesh C. Jinwala, "Improving Route Discovery for AODV to Prevent Blackhole and Gray hole Attacks in MANETs", INFOCOMP, v. 11, no. 1, p. 01-12, March of 2012.
[18] Ngai, E. C. H., Liu, J. and Lyu, M. R. On the intruder detection for sinkhole attack in Wireless Sensor networks. IEEE communication Society matter expert.. Published in IEEE 2006. June. Canada. 3383- 3389.
[19] Teng, Liping. And Zhang, Y. SeRA: Secure Routing Algorithm against Sinkhole attacks for Mobile Wireless Sensor Networks. Second International Conference on computer Modeling and Simulation. 22-24 January (2010). ICCCMS. IEEE. 79-82.
[20] Karlof, C. and Wagner, D. Secure Routing In Wireless Sensor. Networks: Attack and Countermeasures. International conference in, Canada. (2003).