A Detailed Study on Black Hole Attack in MANET

Devendra Kumar
PG scholar,CSE Department
Shri Vaishnav Institute of Technology andScience,
Indore,Madhya Pradesh,
India

Rupali Bhartiya
Reader, CSE Department
Shri Vaishnav Institute of Technology andScience,
Indore, Madhya Pradesh, India

ABSTRACT
Mobile Ad hoc Network is one of the most effective technologies for communication and different types of applications which are working in crucial conditions such as: Army Battle Ground, Disaster Management and similar others but due to completely wireless communication that is not much efficient and a huge number of performance losses are observed in the similar way due to the poor routing strategy, the attackers can also degrade the performance of the network. In this paper the security analysis against black hole attack is performed. In addition of that a brief literature review on recently developed techniques for detection and prevention of black hole is also reported finally based on the different novel solutions a combined effort for detection and prevention of black hole is proposed for further implementation and security of Mobile Ad Hoc Network.

Keywords
MANET, Black hole, Security, Wireless Communication, Routing technique.

1. INTRODUCTION
Mobile ad hoc network is a recent technology, which is basically invented for such conditions where the management of huge infrastructure and maintenance is costly, such as battle ground. MANET (Mobile ad hoc network) can be described by its own characteristics which are that it is self-organizing, mobile communication manner where topologies are dynamically created. Network infrastructure and mobility is an area of new research and development due to its ad hoc nature. Due to mobility of wireless communication two major issues are found in such kind of network i.e. performance and security. Mobile ad hoc has some features which varies it from the other networks which could be in this way like each node has autonomous behavior, the network is capable of multi-hop routing, centralized firewall is absent, creating the network topology dynamic in nature, it has a complete symmetric environment, High user density and large level of user mobility, Nodal connectivity is intermittent. The features of MANET attract researchers in domain of MANET, but some key problems and challenges are also available which limit the performance and security of MANET. Example of MANET is given below in figure 1 which describes its working.

A MANET environment has to overcome certain problems of limitation and inefficiency which consists of some transmission impediments like vanishing, path loss, blockage and interference that add to the susceptible behavior of wireless channels where the nature of the network depends upon the infrastructure that the network holds at that time, it also contains radio band results in reduced data rates compared to the wireless networks therefore the optimal usage of bandwidth is necessary by keeping low overhead as possible, there is dynamic nature of network topology which results in frequent path breaks.

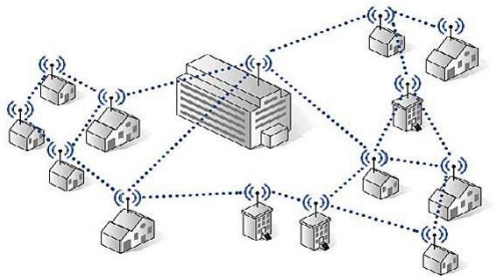

Figure 1 MANET

It has the random movement of nodes which often leads to the partition of the set of connections. This mainly affects the intermediate nodes. MANETs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues (high BER), interference, and frequent breakage in paths caused by mobility of nodes, improved collisions due to the presence of hidden terminals and unidirectional links.

In this paper we described how MANET does work and what its various characteristics are? We studied about black hole which is described in details in section II. Black hole has two aspects detection and prevention of black hole. Our proposed algorithm works for detection, prevention and control to it.

2. HOW BLACK HOLE WORKS
In this section we are going to report some recent and adoptable solution for preventing and securing the network through the black hole attackers. In this attack, a black hole node tries to send fake RREPs to route requests in order to advertise itself as having the shortest path to the destination. These false RREPs deceive the source to divert the traffic of the network toward the black hole node for either eavesdropping or absorbing traffic to drop the data packets.

Cooperative black hole attack occurs when several malicious nodes cooperate to each other in order to absorb data packets. Black hole attack, a malicious node uses its routing protocol in order to With the release of false news, having the shortest path to the destination node. This black hole node advertises its availability of fresh routes irrespective of checking its routing table. In the attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the black hole node reply will be received by the requesting node before the reception of reply from actual node; hence a black hole and forged route is Creation.

When this route is create, now it's up to the node whether to drop all the packets or forward it to the unknown address. In Black hole attack, using routing protocol to an attacker advertises itself as the shortest path to the target device. An attacker watches the routes request in a flooding based routing protocol. When the attacker receives an appeal for a route to the target node, it forms a respond involving of really short route. If the mischievous respond reaches the initiating node before the reply from the genuine node, a fake route gets created. Once the malicious device joins the network itself among the communicating nodes, it is bright to do anything with the packets passing through them. It can crash the packets between them to perform a denial-of-service attack, or on the other hand use its position over the route is the first step of man-in-the-middle attack.

The black hole attack is a well-known security issue in MANET. The intruders develop the loophole to deploy their malicious activities because the route detection process is necessary and predictable. Many researchers have conducted different detection techniques to propose different types of detection schemes.

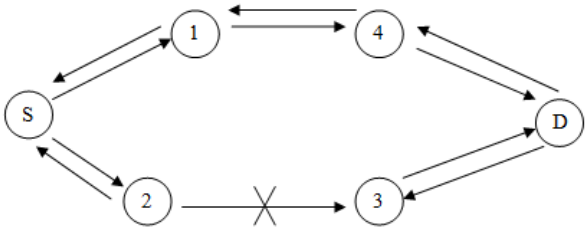

Figure 2 Black hole attacks

For example, in Figure 2, source node S wants to send data packets to destination node D and initiates the route detection process. Suppose that device 2 is a malicious device and it claims that it has a route to the destination whenever it receives route request packets, and straight away sends the reaction to node S. If the reply from the malicious node 2 influences firstly to node S, then node S considers that route detection is finished, than S ignores all other replies and starts to send data packets to node 2. As an outcome, all packets through the malicious node is consumed or lost.

3. RELATED STUDY

Mobile Ad hoc Networks (MANETS) are prone to different types of attacks due to lack of central monitoring facility. The objective is to investigate the effect of black hole attack on the network layer of MANET for different network scenarios. Method: A black hole attack is a network layer attack which utilizes the destination sequence number to claim that it has a fresh and a shortest path to the destination and consumes all the packets forwarded by the source. The various network scenarios of MANETS with AODV routing protocol are simulated using Network Simulator Version 2 (NS- 2) to analyses the performance with and without the black hole attack. The scenarios are created by varying the number of nodes and nodes speed, varying position and number of the black hole nodes and number of flows. The performance parameters like PDR, delay, throughput, packet drop and control overhead are measured. Findings: The black hole attack degrades the network performance. The impact of attack is severe when the attacker is near to the source node, less severe when it is in midway between source and destination and has least effect when it is farther from the source. The overall throughput and PDR increases with the number of flows but reduces with the attack. With the increase in the black hole attackers, the PDR and throughput reduces and close to zero as the number of black hole nodes are maximum. The packet drop also increases with the attack. The overall delay factor varies based on the position of the attackers. Throughput, PDR and control overhead decreases with the network size due to congestion and average delay reduces with black hole attack as the black node sends the Route Error (RREP) without performing any route checking. As the mobility varies the delay and packet drop increases but PDR and throughput decreases as the nodes moves randomly in all directions. Conclusion: The simulation results give a PDR and throughput decreases as the nodes moves randomly in all directions.

An ad-hoc network is a temporary infrastructure less network which is a collection of mobile nodes in the dynamically form. This network is always independent and an isolated network. Due to the limitation power and mobility there is less sufficiency among them. In these wireless networks, the main things like confidentiality, availability authentication, anonymity, integrity to all the users of mobile communication [2]. There are many security attacks in MANET in which these are responsible for the failure in communication from source to destination. Among such attacks black hole attack is one of such serious attacks in MANET. In this paper, we compared the existing solutions and discussed different methods to eliminate the black hole attack in MANET.

Without an establishment of infrastructure or a central network authority Mobile Ad-hoc Networks (MANETs) allow communication of mobile with each other over a network. Due to this condition, the MANETs have dynamic topologies, this case is because the nodes can easily join or leave the network at any time. MANETs are vulnerable to various types of malicious attacks, for this situation a security design perspective is necessary [3].

Ad-hoc on- demand Distance Vector (AODV), which is one of the standard MANET protocols, can be attacked by malicious nodes. This type of malicious attack is a black hole attack that can be easily employed against data routing in MANETs .In this case a black hole node replies to route requests rapidly from the shortest path and the highest destination sequence number. Without any active route and without any specified destination associated with it the black hole node drops all of the data packets that it receives. this mechanism that provides Secure Route Discovery for the AODV protocol in order to prevent black hole attacks. Security is a key feature in MANETs so by using cryptography technique for securing route discovery and data transmission [4].

Wireless sensor networks are mostly maddening in some applications related front line monitoring. The study of selecting cluster heads by the sink is based on the minimization of the related additional energy and residual energy at each node, then the intermediate node selects the near neighbor distance and higher energy sensor node to transmitted the packet [5], if there more than three packet transfer at the same clock so that flooding would be occur to reach the sink between the direct approach and the indirect approach with the use of the nearest cluster head so it block the packet transmitting path behind of black hole region so we preventing such as Average Energy consumption with min Distance vector and minimize dead node occurrence. As the increase of wireless networks, use of mobile phones, smart devices are gaining popularity so the ad hoc network is also

an uprising field. Each device in a MANET is free to move independently in any direction, linking to other devices frequently [5]. Each must forward traffic unrelated to its own use, and therefore be a router. Its routing protocol has to be able to cope with the new challenges that a MANET creates such as nodes mobility, security maintenance, and quality of service, limited bandwidth and limited power supply etc. This paper describes the features, application, and vulnerabilities of mobile ad hoc network also presents an overview and the study of the attacks and their mitigation in routing protocols.

To overcome Black hole attack, a mechanisms such as trust based routing, in intrusion detection system, sequence number comparison and Data Routing Information table (DRI) has been proposed in paper [6]. Trust based On Demand routing mechanism identities and decreases the hazards by malicious node in the path. This paper [6] provides a survey of preventing and identify Ying Black hole attack using trust management mechanism in MANET. A survey of trust based routing protocol in MANET to prevent black hole attack that is caused by a misbehaved node is discussed in this paper. A misbehaved node reduces end to end delivery of packet ratio. To improve packet delivery ratio there is need for identifying the misbehavior nodes dynamically based on trust value.

Black and gray hole attack is one kind of routing disturbing attacks and can bring great damage to the network. Demonstrates an adaptive approach to detecting black and gray hole attacks in ad hoc network based on a cross layer design [7]. In network layer, authors proposed a path-based method to overhear the next hop's action. This scheme does not send out extra control packets and saves the system resources of the detecting node. In MAC layer, a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. Wireless Ad Hoc network is likely to be attacked by the black and gray hole attack. To solve this problem, authors presented a path based method to detect black and gray hole attack. After theoretically analyzing advantages and disadvantages of this method, they proposed an adaptive algorithm to enhance the detection performance [7]. They compare their method to other strategy, and confirm their proposal as successful to provide better detection.

The traditional approaches of securing routing protocols cannot address such insider attacks in DTNs [8]. In this paper, authors proposed a method to secure the history records of packet delivery information at each contact so that other nodes can detect insider attacks by analyzing these packet delivery records. They evaluated the approach through extensive simulations using both Random Way Point and Zebra net mobility models. The results show that their method can detect insider attacks efficiently with high detection rate and low false positive rate. The attack detection is performed based on the analysis of these un-for gable packet delivery records. The scheme used in paper does not rely on a third-party trusted examiner and is easy to apply. Extensive simulation under different mobility models demonstrates that the method proposed in paper can detect black hole attacks effectively with high detection rate and low false positive rate

In paper [9], authors have observed that the performance analysis of one of the most challenging security issue for wireless network i.e. Black hole attack. WiMAX-WLAN interface will play an important role in the NGN (Next generation Network) scenario. This attack is possible in WiMAX-WLAN interface network i.e. in current scenarios. In this type of attack an intruder is a malicious node with less buffer size moving on its defined trajectory and passing from WiMAX-WLAN converter. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This aggressive node advertises its availability of fresh routes irrespective of checking its routing table. In this technique proposed in paper, attacker node will always have the accessibility in replying to the route request and thus intercept the data packet and retain it. On the basis of simulation result they have concluded that black hole attack is possible in WiMAX-WLAN interface network and the performance analysis given idea about packet dropped, delay and throughput at mobile node (malicious node), AP and highly effected client.

The lack of centralized infrastructure in ad-hoc network makes it vulnerable to various attacks. MANET routing disrupts if the participating node start performing malicious activity instead of the intended function. One such specific attack is a black hole attack in which malicious node falsely claiming it as having the fresh and shortest path to the destination. In paper [10], authors propose a protocol for avoiding black hole attack without the constraint of special hardware and dependency on physical medium of wireless network. BAAP (Black hole Attack Avoidance Protocol) forms link disjoint multi-path during path discovery to provide greater path selection in order to avoid malicious nodes in the path using legitimacy table maintained by each node in the network. Non-malicious nodes gradually isolate the black hole nodes based on the values collected in their legitimacy table and avoid them while making path between source and destination, BAAP is a secure routing protocol to defend black hole attack without any requirements of hardware and special detection node. . BAAP also does not require significant changes in the working of existing AODV protocol; however it uses an additional Legitimacy table for avoiding malicious node to grab the path between source and destination.

In Clustering formation through Improved Weighted Clustering algorithm (IWCA) for MANET, author takes various parameters to create a metrics for formation of cluster [11]. It represented an automated trust management scheme for MANETs that uses a packet drop rate (PDR), packet misroute rate (PMR), packet modification rate (PMOR) three parameters to assess the trustworthiness of nodes. In this articles IWCA improved the trust of cluster formation followed by malicious node removal from the cluster.

4. PROPOSED WORK

In this section we are addressing the key issues and challenges for black hole attack prevention in MANET. In addition of that a solution is also proposed which will be helpful for improving the network performance and also used to prevent the attacker nodes.

4.1 Problem Domain

The given source based trusted AODV routing protocol for MANETs approach is efficient and adoptable, but security is not give better results [1]. In source based trusted AODV routing technique many times it removes welfare nodes from network whenever it does not reply control messages to previous sender node due to some technical issues. In addition of that this article is focused on addressing the performance issue in MANET. This may not much involve in providing security.

In this context, the trust value based model is also available in this concept to improve the security. That is not much

effective due to improper selection of malicious nodes. Therefore some improvement over this proposed method is required to provide the security in MANET.

4.2 Solution Domain

In a MANET when we using ad-hoc types of routing ,if nodes want to communicate then the route search has been start, there are different types of packets in a MANET such as data packets and routing packets routing packets are which is used for path searching from source to destination so the source send a routing packets known as RREQ packets which also known as request packets contain all the information about source and destination and these packets flood to his neighbors nodes then they send it to their neighbors nodes so these packets travel hole network and then when they find out the destination they reply message were start to sending form destination ends and a route has been establish .The other types of packets are data packets which contains data .

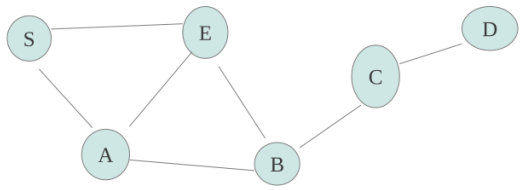

Figure 3 Network Scenario

In above picture shows a MANET where solid lines shows the paths between all the nodes ,S is our source and D is our destination when source S want to send data it start sending RREQ packets and then D reply to other networks nodes when sending nodes received these packets it starts sending data packets from its shortest path. In our work we maintain a history table which contain send packets ,received packets and dropped ratio which is calculated by using send packets/ received packets for every node in our network than all the values of dropped ratio we calculate a mean value of all the drop ratio, we set it to our threshold value and than compares it to all the drop ratio of every node for finding out malicious node. we design an algorithm which is depend on the dropped ratio of every nodes if the threshold value is less than drop ratio of nodes that nodes set to 1 ,then this nodes are set to know and data sending is continue , else the threshold value is more than drop ratio of nodes than these node is set 0 and called its suspected nodes and then we check by using other method we can set it to finally as know or unknown node ,in these method we send RREQ packets 3 times to these nodes for testing to it, if these packets are dropped than it set to be unknown for our network if the condition false and packets are not dropped than the node are safe to communicate to other nodes .

The Mean value is the 'average value' of drop ratio of the node. Which is calculated by sum of all the drop ratio values divided by total number of drop ratios.

Find the mean of following, 0.7, 0.8, 0.2, 0.3, 1.0, 0.0, 0.9, 0.5

The Median is= 0.5 .

Here we apply a neural network for evaluating the above table thus we the above table is provided as input for neural network and the neural network is trained using the given values. For training of neural network required some important parameters such as number of training cycle, input layers, number of training patterns and learning rate.

Table 1 Evaluation Table

Nodes	Received packets	Sent packets	Drop ratio
A	5	7	0.7
B	4	5	0.8
C	1	4	0.2
D	3	10	0.3
E	8	8	1.0
F	0	2	0.0
G	8	9	0.9
I	3	6	0.5
Threshold value=0.5			

Neural network uses the number of training cycles for correcting the error in output omitted. That error is evaluated as

Error = actual output – output found

And these values are adjusted in the neural network weights; the activation function of a node defines the output of that node given an input or set of inputs. The output calculation is performed as the below given function [12]

$$y = \sum_{i=1}^{n} w_i x_i$$

n = the number of input units to the neuron
i = the i^{th} weight

- = the i^{th} input value to the neuron

5. CONCLUSIONS

Reporting a survey on MANET and their security flaws concerned with the black hole attack. In addition to this during the research study we observed the various techniques by which black hole are prevented. This study based on method in literature for MANET black hole attack detection. We have proposed a method in which mean value of packet drop ratio is used for attack detection and use this method we can prevent the network in a more efficient way. we concentrated on how black hole can be prevented by developing a solution with the help of Wireless Communication Algorithm and in near future this issue of black hole attack can be sorted out by using NS2.

6. ACKNOWLEDGMENTS

After the completion of this paper, work are not enough to express my feeling about all those who helped me to reach my goal; feeling above this my indebtedness to The Almighty for providing me this moment in life.

It's a great pleasure and moment of immense satisfaction for me to express my profound gratitude to Mrs. Rupali Bhartiya, Reader, Computer Science and Engineering Department SVITS Indore, whose constant encouragement enabled me to work enthusiastically. Their perpetual motivation, patience and excellent expertise in discussion during progress of the dissertation work have benefited me to an extent, which is beyond expression. Their depth and breadth of knowledge of Computer Engineering field made me realize that theoretical knowledge always helps to develop efficient operational software, which is a blend of all core subjects of the field. I am highly indebted to them for their invaluable guidance and ever-ready support in the successful completion of this dissertation in time. Working under their guidance has been a fruitful and unforgettable experience.

I wish to acknowledge my deep sense of gratitude for Dr. V.N. Walivadekar, Principal SVITS Indore for providing necessary infrastructure and help to complete the project work successfully.

I express my sincere thanks and gratitude to Dr. Anand Rajavat, Head, Computer Science and Engineering Department, SVITS Indore, who took care about imparting expert knowledge for design and development of project.

7. REFERENCES

[1] R.Parthasarathy, A.Pravin Renold, Source based Trusted AODV Routing Protocol for Mobile Ad hoc Networks, International Conference on Advances in Computing, Communications and Informatics (ICACCI-2012).

[2] Christeena Joseph*, P. C. Kishoreraja, Radhika Baskar and M. Reji, "Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios", Indian Journal of Science and Technology, Vol 8(29).

[3] Nakka Nandini, Reena Aggarwal, "Prevention of black hole attack by different methods in MANET", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue.

[4] Hansraj Bhakte, Prof. Rahul Kulkarni, "Prevention Of Black Hole Attacks In AODV- Based Manets Using Secure Route Discovery", Journal of Multidisciplinary Engineering Science and Technology (JMEST).

[5] Rajni Rani, Ms. Preethi Dolly, Mr. Devender Kumar, "Black Hole Prevention & Detection under Average Energy Consumptionin WSN", IJCSMC,Vol.4.

[6] U.Venkanna1, R.Leela Velusami, Black Hole Attack and Their Counter Measure Based On Trust Management in Manet: A Survey, Int. Conf., on Advances in recent technologies in communication and computing 2011.

[7] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network, 1550-445X/10 $26.00 © 2010 IEEE.

[8] YanzhiRen, MooiChooChuah, Jie Yang, Yingying Chen, Detecting Blackhole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording, 978-1-4244 7265-9/10/$26.00 _c 2010 IEEE.

[9] Rakesh Kumar Jha, Upena D Dalal, Idris Z. Bholebawa, Performance Analysis of Black Hole Attack on WiMAX-WLAN Interface Network, 978-0-7695-4872-2/12 $26.00 © 2012 IEEE.

[10] Saurabh Gupta, SubratKar, S Dharmaraja, BAAP: Blackhole Attack Avoidance Protocol for Wireless Network, 978-1-4577-1386-611$26.00©2011 IEEE.

[11] Neha Gupta, Rajeev Kumar Singh, Manish Shrivastava, Cluster Formation through Improved Weighted Clustering Algorithm (IWCA) For Mobile Ad-hocNetworks,978-1-4673-5999-3/13/$31.00 ©2013 IEEE.

[12] James A Anderson, An Introduction To Neurl networks, MIT Press , 1995.

[13] Fidel Thachil, K. C. Shet, "A trust based approach for AODV protocol to mitigate black hole attack in MANET", International Conference On computing Science 2012.

[14] Karim El Defrawy, Member, Gene Tsudik, Senior Member, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", Computer Science DepartmentUniversity of California, Irvine, CA, USA.

[15] E.A.Mary Anita, V.Vasudevan, A.Ashwini, "A Certificate-Based Scheme to Defend Against Worm Hole Attacks in Multicast Routing Protocols for MANETs", 978-1-4244-7770-8/10/$26.00 ©201 0 IEEE.

[16] Quansheng Guan, F. Richard Yu, Shengming Jiang and Victor C.M. Leung, "A Joint Design for Topology and Security in MANETs with Cooperative Communications", 978-1-61284-231-8/11/$26.00 ©2011 IEEE.