THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

A Review on Black Hole Detection Technique In Mobile Adhoc Network

Robin Prakash Mathur
Asst.Professor, School of Computer Science & Engineering
Lovely Professional University
Punjab, India
mathur.robin@gmail.com

Sharanpreet singh
Research Scholar, School of Computer Science & Engineering
Lovely Professional University
Punjab, India
spsingh.decentboy@gmail.com

Abstract: MANET is a promising and rapidly growing field in recent times in the field of wireless networks based on a self-organizing and rapidly deploying network. Mobility and wireless communication has become significant area of research in modern computing environment. With the emergence of technology, the rise of various types of attacks for controlling the technique has also increased. Various efforts are laid down by the researchers time to time to provide the efficient solutions to overcome such attacks and mitigate the risk of compromising the communication network. One of the key attacks is black hole attack in which one communication node claims to be having the shortest path from the source to the destination by replying to the route request packet of the sender node. In this paper, the review of various black hole detection techniques has been presented and working of the techniques are discussed.

I. INTRODUCTION

Mobile Adhoc Network (MANET): A mobile ad hoc network is a decentralized autonomous system of the mobile nodes which are connected to each other via wireless links and all nodes co-operate with each other by transferring data packets to each other in the network. It is a simple network with limited number of nodes which act as both hosts as well as the routers although a mobile ad hoc network do not require any type of base station or an access point or routers to deploy which is the key feature of MANET. It is not necessary that the source and the destination nodes are always in a direct connection with each other so they need the help of the other nodes within the same network, to make the communication possible. There is no central control device which can control the data transfer and processing of the different nodes in MANET so it provides less security and leads to more chances of data loss within the network. But also on the other side it provides facilities like ease of deployment and faster speed of deployment. Due to the nature of trusting the other nodes for communication withifn the network the mobile ad hoc networks are highly vulnerable to various attacks which give us a vast area to research on. Not just that, there are several other issues as well which are discussed further.

II. VARIOUS BLACK HOLE DETECTION TECHNIQUES

Black hole detection with a new control packet [1]: The paper contains the details about variety of attacks that may occur inside a mobile ad hoc network. A black hole attack is a denial of service type attack that stops the data transmission by dropping packets. In this approach, the modification in the route detection mechanism is done. The source node sends RREQ packet along with another CREQ i.e. Confirmation Route Request packet towards the next hop to the node which generates a RREP message. The next hop node then receives a CREQ packet and replies to the source with the conformation that does the destination's path is in its routing table or not and reply with a CREP i.e. Conformation Route Reply Packet. The validation is done with the help of the next node. In case if the next hop is also malicious then the source waits for more than one route reply packets and then check for a common node's presence in the two paths and rely on the path if it is there. The other drawback of this approach was that it consumes more time because it waits for multiple RREP packets to arrive.

Study of different attacks and performance parameters [2]: MANET is that type of network which allows different nodes to join the network and trust that node for data transmission without any verification because of lack of central management. Due to this property, MANET is vulnerable to many types of attacks which are explained in this paper, such as Black hole attack, Jellyfish attack, and Neighbor attack. The first two attacks are common in nature except that Black hole drops the packets and Jellyfish delays the packets and in the Neighbor attack the AODV protocol is modified as no node will be sharing their ID in the route detection so that the malicious node can make the others believe that it is directly connected to the destination.

A timer based approach for black hole detection [3]: In this approach, a max_trust value is assigned to every node in the network at the time of their joining. The nodes will not do any data transmission with the nodes which have trust value less than min_trust value. These trust values are dependent on the performance of the nodes in the process of data transmission. When source node starts forwarding the data packets after the route discovery, it provides a unique additional number to the nodes. When the node N starts forwarding the packets it starts a time to live value and adds it to each packet. When this TTL value expires, the node N enters the promiscuous mode and sees if the next node has received the packet or not. If the packet is not there then the node (N) decreases the trust value of that node and if the next node keeps on dropping packets like that then the trust value also kept decreasing and once the trust value is less than min_trust value then all the other nodes put this node into their blacklist table.

Black hole detection on the basis of intrusion detection system [4]: An intrusion detection system is the one which detects the behaviour of a network or a scenario and compares it with the normal behaviour which is

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

supposed to be happening in the system. If the behaviour is found to be different or uneven then alarm is sounded to notify others in the system. This intrusion detection system is implemented in the MANET with some modification like a counter is set on the RREQ packet and instead of unicasting the RREP is broadcasted with a counter on it to notify the sender. The neighbouring nodes keep on checking the behaviour of the other nodes in their range for anomaly detection. An IDS agent in order to keep track of the network keeps an audit data collection. Previously information about the network and detected anomalies are also stored. The limitation of this approach is that it is time consuming.

Secure AODV Black hole prevention [5]: In this paper, a new approach is provided in order to prevent the black hole node by simply ignoring the first route reply packet that is received by the sender and selecting the next RREP packet received for data transmission. It may have increased the time taken for the data transmission but on the other hand the Black hole prevention is done at a high success rate at a very little cost.

Assessment based detection of Black hole attack [6]: In this work, the recognition of the Black hole node is prepared on the basis of time value. This time value is calculated on the basis of connection establishment and breakage. All the nodes in the MANET are mobile in nature, when a new node comes inside the range of the source node its time of joining is taken and as soon as the node leaves the series of the source node, again its time is taken and after getting these two time values their difference is taken. This difference is called the hint value and this hint value is further compared with the threshold value which was set earlier. If the hint value is not as much of than the threshold value then the particular node is reflected as the Black hole node else it is a trustworthy node. The performance parameters are there with an improved packet delivery ratio and throughput.

In paper [7], black hole attack on AODV routing technique has been discussed and shows how single and cooperative black hole attack happens in the network.

A new approach for black hole detection “BRAVO” [8]: In this approach, two additional fields are added to the routing table which are credit and counter. A credit value reflects the level of trust as an integer value. Its value is initialized with a formula i.e. K*Hop Count. A counter is added to the table initially with value 0. As the data packets are transmitted, its value kept increasing and once the value reaches to a certain value, the credit value is decreased by 1 and the counter is again set to 0. On receiving the packets from the previous node S, the next node R checks whether the next node to the source is S or not and this way it comes to know if the node S is trustworthy or not.

A cooperative bait detection approach to detect collaborative black hole attacks in MANET [9]: In this approach, the neighboring node is considered as bait by source node to entice the black hole nodes. The

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

basic working is that, the source node asks for the path to the network about the destination which is a node from its neighborhood at a one hop distance. The system is triggered only when there is an alarm about something malicious is happening in the network. It means when the source node receives many RREP packets from paths other than the path of the bait node then it is definitely coming from a malicious node. Now a reverse tracing program is triggered in which the path from source to the destination is divided into two paths i.e. temporary trusted path and the non-trusted path. In reverse tracing, the source node sends a test packet and a recheck packet and goes to the promiscuous mode to listen to the network for the detection of the malicious node. The main disadvantage is that it consumes lots of time and resources and also it has to discard the bait path permanently means that sender cannot send any data packet to the direction of the bait node because this side is not verified as the bait is chosen randomly.

In detection of cooperative black hole attack [10], the routing information table is another approach which is very helpful in the detection of the cooperative black hole attack. In this table, there are 3 columns named as From Node, Through Node and Through Any Trustful node. In the columns there are integer values where 1 stands for True and 0 stands for False. This table is created at each node having information of these three columns about each node in the network presently available. The 1st column indicates whether the node has transmitted data from this other node previously or not. The 2nd column indicates whether the node has received data from this other node previously or not. The 3rd node indicates whether this other node has been used for data transmission by other trustful node or not previously. On the bases of these values the source node selects the other node for data transmission.

Detection of cooperative black hole attack using DRI table [11]: In this paper, a data routing information table is used which is stored at each node containing value to the columns From, Through and Check Bit. These columns are filled with values either 0 or 1 where 0 means false and 1 means True. The check bit column is filled with the help of sending a probe packet to a particular node and check if the node receives the packet or not and on the basis of this process the third value is given to the table.

In GAODV [12], the gratuitous AODV is new approach to detect black hole node. In this approach, the source node and the destination nodes use some control packets to detect the black hole node as the RREP is generated by the intermediate node (IN), the IN not only send the RREP to the source but also generates a CONFIRM packet and send it towards the destination. When the destination receives the CONFIRM packet from the IN, it then waits for the CHCKCNFRM packet from the source. After receiving these two packets, the destination replies to the source by unicasting a REPLY CONFIRM packet. Now all these new control packets carry some important information. Since, the black hole node does not know the actual location of the destination, it cannot send a CONFIRM packet towards destination and when the destination receive

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

only CHCKCNFRM packet from the source and do not get any packet from the IN it do not forward the REPLYCONFIRM packet to the source and that is how the black hole node is detected. Now these new control packets store the information regarding the source address and the id of the IN. These addresses are used to detect malicious nodes in the network.

Detection of cooperative black hole attack using Clock Synchronization and Relative Velocity Distance [13]: For the discovery of cooperative black hole nodes, broadcast synchronization method is used in this paper. Basically, all the clocks are synchronized with each other. The internal clock time of the network is compared with the external time clock and both the times are compared with the standard threshold time clock given that the clock time of a node is always greater than the threshold time during initialization. There is another method imposed for detection of black hole nodes because sometimes the clock synchronization method fails when worms are present in the network. This new method is, calculating the relative distance from the source to the destination and making it the threshold distance and then comparing it with the actual distance from the source and the destination. Some normal cases and abnormal cases are explained as an example to explain these two methods for the detection of the cooperative black hole nodes in the network.

A novel approach for black hole node detection using MDE [14]: In this approach, when for the first time the node is receiving beacon, it compares it with the other beacon signals received from all the neighbours and check if the destination address is changed or not. If the destination address is changed then the last address of the node from the beacon is changed to malicious and all the other nodes are notified. After the updation, a new MN address (non-mutable) field is added to the beacon with the property that the data in this field can only be updated and can never be altered. Based on this property the changed destination addresses of the nodes are analysed for detection and removal of the black hole nodes from the network. For authentication purpose, the concept of public key and private key is used.

A new approach for black hole detection [15]: In this paper, the concept of the data routing information table is used for the detection and prevention of the black hole node. The final step of the process is modified from the former approach. When a node sends a RREP packet back to the sender, it adds two extra addresses i.e. Next Hop Node (NHN) and Previous Hop Node (PHN) along with the packet with their DRI values inside the packet. These DRI values are checked for the value to be 1 in at least Through part of the routing table column and if it is 0 then there must a 1 value in the From part of the routing table column. If any of the values are 0 then the RREP generator node has to send a data packet to the NHN or PHN based on their value to convert it into 1 means YES means the communication did takes place. When both the values are 1 only then the RREP node sends the information back to the sender for data route creation.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

In this approach [16], it is another data routing information table based approach with a slightly changed crosschecking mechanism. In this approach, using rendezvous phase a nonce key is shared i.e. two random numbers are shared among nodes where RREP packet is generated. Based on the time constraint, the neighbouring nodes enters the values in the DRI table which haven't received the acknowledgment 0 or 1. After getting entries in the DRI table by the adjacent nodes, these values are verified using link verification method i.e. by sending ECC signature and two-nonce.

In approach [17], it is a support vector machine (SVM) based approach where SVM accepts set of input data and the behaviour of the nodes is observed. Packet delivery ratio (PDER), packet modification ratio (PMOR) and packet misroute rate (PMISR) are the various terms used in this research. For the detection of the malicious nodes, the system detects the behaviour of the nodes based on these mentioned values and with the help of SVM classifier the nature of the nodes is classified, integrating with the MANET. Firstly, all metrics collected are saved as XML file. Then extracting the XML files using Dynamic Object Module and uses these values as input for SVM

Anomaly based intrusion detection of the black hole node in MANET [18]: In this approach, a monitoring node is used for the detection of the abnormalities in the network and detecting the malicious nodes based on the observations. There are some basic rules which are needed to be followed in order to execute this approach. Firstly, the monitoring node holds a unique ID so that it can easily be illustrated from the other nodes in the network. It can cover all the nodes in the neighbour. It observes the behaviour of the neighbouring nodes at the network layer with the help of anomaly based intrusion detection. If the malicious node is encountered, it alarms the other nodes in the network. The detection process of the malicious nodes is very simple. As the monitoring node has the power to monitor the whole topology of the network, it checks regularly whenever some data packets are travelling inside the network, the packet at each node before receiving and after forwarding is observed and compared. If the packet has a slightest change, the monitoring node intimate it to the sender and the packet is resend and that node is captured. If this step is successfully executed it means that the packet is safely reached at the destination.

Secure routing to prevent black hole attack in MANET [19]: In this technique, the nodes are using the promiscuous mode to overhear the other nodes to check whether the packet is received or not. When a node replies to a route request packet then the node prior to the RREP node sends a plain data packet to the next to next hop of the RREP node and goes to the promiscuous mode to check whether the packet has been transferred to that node or not through the RREP generating node. If the plain data packet is not present at the next to next hop then the RREP generator node is malicious else the node is clean. The flow chart and the algorithm with graphical simulation of the output are given to make it clearer to understand.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Trust based security schemes a review [20]: In this paper, several trust based research papers are collectively explained along with the details of how the trust is actually created among nodes in a mobile adhoc network and how this value is used for future data transmissions. Basically, the nodes have to trust the other nodes initially and then on the bases of their efficiency a trust value is given to the nodes for future use.

Securing the data packets using asymmetric keys for data encryption and decryption [21]: In this paper, clustering technique is used where each node generates its public and private keys and sends only public key to the cluster head. When the process of communication starts, the sender node first conveys the message to the cluster head and asks for the public key of the destination node. If the destination node is also in the same cluster then the work is easier else the cluster heads communicate with each other to get the public key of the destination node and sends it to the source node. The source node encrypts the data using this public key and send it to the cluster head on the other side, the destination node uses its own private key to decrypt the message and hence the data is secure.

In paper [22], adhoc on-demand multipath secure routing (AOMSR) method is introduced. It is based on permutation acknowledgement which helps to detect black hole node in the network. There are several paths between the source node and the destination node which all are used in this approach to discover out the malicious node path. The data structures used are path number, permutated acknowledgement number, total number of paths and type of message. The sender sends each path a message with its path number and permutated acknowledgement number along with it. When the destination receives these messages, it stocks all the applicable entries in the table and via pre-decided paths sends back the permutated acknowledgement. The sender node re-checks all the values to see if the values are received correctly. If it is true then there is no malicious node in the paths. But if there are some changes in the values then there must be a malicious node in the path which can be figured out with the help of PN number. The algorithm for the above approach is mentioned with the detailed description of its working explained.

In approach [23], each node in the network heeds to the neighbouring nodes in the promiscuous mode. Each node observes the behaviour of the other nodes in order to see if the data packets are transferred in good health or not. The information is compared with the information stored in the knowledge table at each node. These two values must be same in order to confirm that the node is legitimate node. If the values are not same then the given node gaps for a particular extent of time and tries to find out the reason of packet dropping. The reason can be figured out with the help of the algorithm given in the paper. The node is stated as malicious if the threshold is reached due to packet dropping. Also the node checks whether the subsequent hop node is the target node or not and TTL value is also checked in order to wait for the packet to arrive due to delay.

Securing network layer using C-Scan energy efficient protocol [24]: A previously introduced E2-SCAN scheme is modified into Conditional-SCAN with a new strategy for the token renewal. In this approach, promiscuous mode is used by all the nodes to hear the other nodes. Monitoring activities takes place among the nodes in the network. To gain the network access, each node needs to have a token with a valid sign with the fields i.e. owner id, signing period and expiration period. When a node wants to renew its token, it directs a token request packet comprising old token ID and the current timestamp to the neighbouring nodes.

In approach [25], the modified extended data routing information table, a modification in the DRI table is done in this paper in order to enhance the capability of the black hole node detection and providing more promising security to the network. In this MEDRI table, we have eight fields with two older and six new fields. The third column is CTR means counter. The purpose of this column is to count how many times the node has behaved maliciously. The fourth column is BH that indicates the latest reaction of the node either malicious (1) or not (0). The fifth column is Timer, that will be used to consider a node malicious or not. The sixth and seventh columns are used for calculating the data packet size at the source and at the destination, respectively. The last or the eighth column, which is Result, uses a Boolean value (Yes/No) for the result of the comparison of the previous two fields. On the basis of these values a malicious node is detected in the network.

CONCLUSION

The study of various black hole detection techniques has been presented in this paper. Sufficient research has been done in this topic but still lot of scope is there to improvise the performance of the black hole detection.

REFERENCES

[1] BOUNPADITH KANNHAVONG, HIDEHISA NAKAYAMA, YOSHIAKI NEMOTO, and NEI KATO, "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS," 2007.

[2] Hoang Lan Nguyen and Uyen Trang Nguyen, "A STUDY OF DIFFERENT TYPES OF ATTACKS IN MOBILE AD HOC NETWORKS," *25th Canadian Conference on Electrical and Computer Engineering (CCECE)*, p. 6, 2012.

[3] Nidhi Choudhary and Dr. Lokesh Tharani, "Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism," *SPACES-2015, Dept of ECE, K L UNIVERSITY*, p. 4, 2015.

[4] Kriti Patidar and Vandana Dubey, "Modification in Routing Mechanism of AODV for Defending Black hole and Wormhole Attacks," 2014.

[5] Ashish Kumar Jain and Vrinda Tokekar, "Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks," *2015 International Conference on Pervasive Computing (ICPC)*, p. 6, 2015.

[6] Pooja and R. K. Chauhan, "AN ASSESSMENT BASED APPROACH TO DETECT BLACK HOLE ATTACK IN

MANET," *International Conference on Computing, Communication and Automation (ICCCA2015)*, p. 6, 2015.

[7] Rakesh Ranjan, Nirnemesh Kumar Singh, and Ajay Singh, "Security Issues of Black Hole Attacks in MANET," *International Conference on Computing, Communication and Automation (ICCCA2015)*, 2015.

[8] Ermanno Guardo, Giacomo Morabito, Girolamo Catania, Agatino Mursia, and Ferdinando Battiati, "BRAVO: A Black-hole Resilient Ad-hoc on demand distance Vector rOuting for tactical communications," *2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, p. 2, 2014.

[9] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," *IEEE SYSTEMS JOURNAL*, vol. 9, p. 11, March 2015.

[10] Ms. Gayatri Wahane and Ms. Savita Lonare, "Technique for Detection of Cooperative Black Hole Attack in MANET," *IEEE - 31661*, p. 8, July 2013.

[11] Ankur mishra, Ranjeet Jaiswal, and Sanjay Sharma, "A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network," p. 6, 2012.

[12] Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathur, and Prashant Khurana, "GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs," *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, p. 6, 2013.

[13] Harsh Pratap Singh and Rashmi Singh, "A Mechanism for Discovery and Prevention of Coopeartive Black hole attack in Mobile Ad hoc Network Using AODV Protocol," p. 8, 2014.

[14] Vaithiyanathan , Gracelin Sheeba. R, Edna Elizabeth. N, and Dr. S. Radha, "A Novel method for Detection and Elimination of Modification Attack and TTL attack in NTP based routing algorithm," *2010 International Conference on Recent Trends in Information, Telecommunication and Computing*, p. 5, 2010.

[15] Ali Dorri and Hamed Nikdel, "A New Approach for Detecting and Eliminating Cooperative Black hole Nodes in MANET," *IKT2015 7th International Conference on Information and Knowledge Technology*, p. 6, 2015.

[16] Gayatri Wahane, Ashok M. Kanthe, and Dina Simunic, "Detection of Cooperative Black Hole Attack using Crosschecking with TrueLink in MANET," p. 6, 2014.

[17] Meenakshi Patel and Sanjay Sharma, "Detection of Malicious Attack in MANET A Behavioral Approach," p. 6, 2012.

[18] Shivani Uyyala and Dinesh Naik, "Anomaly based Intrusion detection of Packet Dropping Attacks in Mobile Ad-hoc Networks," *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, p. 4, 2014.

[19] Ashutosh Bhardwaj, "Secure Routing in DSR to Mitigate Black Hole Attack," *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, p. 5, 2014.

[20] S. Sivagurunathan and K. Prathapchandran, "Trust based Security schemes in Mobile Ad Hoc Networks – A Review," *2014 International Conference on Intelligent Computing Applications*, p. 5, 2013.

[21] Adel ECHCHAACHOUI, Ali CHOUKRI, Ahmed HABBANI, and Mohamed ELKOUTBI, "Asymmetric and Dynamic Encryption for Routing Security in MANETs," p. 6, 2014.

[22] Dhaval Dave and Pranav Dave, "An Effective Black Hole Attack Detection Mechanism using Permutation Based Acknowledgement in MANET," p. 7, 2014.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[23] Ayesha Siddiqua, Kotari Sridevi, and Arshad Ahmad Khan Mohammed, "Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm," *SPACES-2015, Dept of ECE, K L UNIVERSITY*, p. 5, 2015.

[24] Sanjay K. Dhurandher, Isaac Woungang, and Issa Traore, "C-SCAN: An Energy-Efficient Network Layer Security Protocol for Mobile Ad Hoc Networks," *2014 28th International Conference on Advanced Information Networking and Applications Workshops*, p. 6, 2014.

[25] Vani A. Hiremani and Manisha Madhukar Jadhao, "Eliminating Co-operative Black hole and Grayhole Attacks Using Modified EDRI Table in MANET," p. 5, 2013.