A Snapshot of Black Hole Attack Detection in MANET

Moirangthem Marjit Singh
Department of Computer Science & Engineering
North Eastern Regional Institute of Science & Technology
Nirjuli, Arunachal Pradesh,India

Ankita Singh
Department of Computer Science & Engineering
North Eastern Regional Institute of Science & Technology
Nirjuli, Arunachal Pradesh,India

Jyotsana Kumar Mandal
Department of Computer Science & Engineering
University of Kalyani
Nadia,West Bengal, India

ABSTRACT

Black hole attack is a very common type of security attack found in Mobile Adhoc Network (MANET). In Black hole attack, the malicious node attracts all the data packets towards it using some false means and affects the data transmission in many ways, such as dropping of the packets. Black hole attack is vulnerable to security in MANET routing protocol. The paper focuses to provide a snapshot on various methods of detecting black hole attack in MANET and critically reviews them.

General Terms

MANET Security

Keywords

Network security, Black hole attacks, MANET

1. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes which do not have a fixed connectivity with the fellow nodes rather find a connection to the desired node as and when required, hence they are referred to as Ad-hoc networks [1]. This eliminates the need of periodic link maintenance. Every message travelling through a network has a source and a destination, apart from this, every intermediate node traversed by the message acts as a router, which forwards the packet which has to go to another node through it. Various routing protocols have been proposed for MANETs, in which AODV routing protocol has gained maximum interest. Many of the routing protocols are susceptible to numerous attacks; Black hole attack is one of them.

Black hole attack is assumed analogous to the black hole existing in the universe in the way that the malicious node attracts all the data packets towards itself through some false means and affects the data transmission in many adverse ways, such as, the malicious node drops the obtained packets [2]. AODV being one of the most widely accepted routing protocol for MANETs many black hole detection techniques are based on AODV. There are two types of black hole attack namely single black hole attack and cooperative black hole attack [6]. In single black hole attack there is only one malicious node and on the other hand cooperative black hole attack is that in which many malicious nodes collaborate together to damage the network more seriously.

In the AODV [3] protocol whenever a node needs for a route to transmit its data to a particular destination, it requests for the route through a route request (RREQ) message, which is broadcasted to all its neighbors. Each neighboring node acts as an intermediate node and responds with a route reply message (RREP) if it has a fresh route to the destination else it rebroadcasts the message to its neighbor and in this way the request reaches the destination. Every RREQ message contains a Sequence Number (SN) which helps the source to decide the most recent route to the destination. The literature survey suggests that various methods have been proposed to detect black hole attack some of which are discussed here.

2. DETECTION METHODS

2.1 Neighborhood Based Detection Method

Sun et al [4] have proposed a neighborhood based detection method to detect the existence of black hole attack in the network and an efficient routing recovery protocol to route the packets to the correct destination which helps to mitigate the black hole attack. The authors use the neighbor set of a node as a metric to verify the identity and authenticity of the node. The authors conducted two different experiments to support the correctness of the chosen metric, in which the first one showed that the neighbor set of a node do not change much during the route discovery phase and the second one demonstrated that the probability that two nodes have the same neighbor set is to low less than 0.00001 [4].

Using the neighbor set as the metric the authors have proposed a method which can detect and mitigate the black hole attack. The method consists of two parts namely *detection* and *response* [4]. In the detection phase, the source node collects the neighbor set of the destination node. To accomplish this task **t**he authors have introduced two control packets namely RQNS *(Request_Neighbor_Set)* and RPNS *(Reply_Neighbor_Set)*. On receiving the reply for a route form an intermediate node, the source generates a RQNS packet and unicasts it to the replying node, which sends back RPNS. Having received more than one RPNS, the source node compares the difference between the two neighbor sets and if the difference between the sets is found greater than a predetermined threshold value then the source node concludes the presence of black hole attack. In the response phase, the source node uses the cryptography methods to choose the correct destination. The authors have claimed that their proposed protocol is more effective as it requires less encryption/decryption operations than other techniques which depend on cryptographic techniques. Simulation results in [4] show that the detection rate is above 93% and the use of routing recovery mechanism increases the throughput by at least 15% and the false positive rates were also reduced drastically.

2.2 PDRR Based Detection Method

The concept of analyzing the Packet Drop Ratio (PDRR) to detect the abnormal behavior of the nodes to detect the black hole attack is reported in [5], where PDRR is the performance metric. The authors have calculated a maximum Packet Drop Ratio for an attack free network and set it as the *threshold value.* The authors propose that under normal working condition the calculated PDRR is always smaller than the threshold. Otherwise in the case of an attack the PDRR is greater than the threshold value and hence a node can detect the black hole attack.

2.3 Advanced DRI Table Based Method

An improved AODV protocol using advanced DRI (Data Routing Information) table, deployed with an additional *check bit* was proposed by Mishra et al [6]. This method deals both the single black hole attack and the cooperative black hole attack. The method provides four procedures to enhance the security of the network.

1. *Neighborhood data collection and local malicious node detection:* In this procedure each node keeps a check on the packet transmission of the neighboring nodes by storing the data forwarding information of each neighbor and on detecting abnormal behavior of a malicious node, it initiates a *local anomaly detection* [6] procedure to detect the malicious node.

2. *Finding trusted node to destination and complete elimination of co operative black hole:* To find the trusted node, the source node demands the DRI tables from the destination node and the intermediate nodes. The source node then examines the received DRI table to find the trusted node depending on the value of the *check bit* [6].

3. *Establish secure path to destination:* The nodes with check bit '1' are assumed to be the trusted node [6]. The DRI entries of such nodes are checked further to see other nodes with their check bit as 1 and following the sequence a secure path is found towards the destination.

4. *Global alarm arising and blacklisting malicious nodes:* The nodes with their check bit as '0' are marked as blacklisted as malicious node.

2.4 Using Promiscuous Mode

Sharma and Gupta [7] present a secure AODV routing protocol which is a modified version of the existing AODV routing protocol to enhance its security against the vulnerable attacks using the *promiscuous mode* [7] of the nodes. In the promiscuous mode a node can overhear the communication of its neighbors even though it is not involved directly in the conversation [7]. In this protocol when a intermediate node responds to the source node by sending a RREP, at that moment its neighboring node which is just before this node in the path from source to destination starts acting in promiscuous mode and sends a plane packet to the replying node and checks whether or not the node sends the plane packet to the intended receiver. If the node forwards the packet it is assumed to be a trust worthy node else it is marked as malicious and the network is alarmed about it.

2.5 Using Path Redundancy and Sequence Number Comparison

Raut and Chede [1] have proposed two techniques for detecting black hole attack. The first method utilizes the concept of redundancy of paths available to the source node to reach a particular destination. Since redundant paths to reach a destination are possible hence the source node after requesting for a route through the RREQ packet waits for the response from more than one node to verify a secure route. On receiving a RREP (Route Reply) the source node extracts the path and compares the two routes, it is observed in the case of MANET that two paths to the same destination have certain hops in common, thus if the two responding nodes have certain common hops are considered to be secure and reliable to transmit the data. In the second method the traditional sequence number comparison is done to ensure the correctness of the path. These methods can mitigate a single black hole attack but cannot tackle the collaborative black hole attack, in which many malicious nodes collaborate together to carry out network attacks.

2.6 Using Additional Route Reply (RREP)

Vipin et al [8] have proposed an approach in which the source node stores all the route reply messages received within the allowed time slot to analyze the data and find the most fresh and secure route to the destination. This is an additional method augmenting the normal AODV protocol and to implement this the authors have used an additional function named *preprocess RREP( )* [8]. The defined function contains a table to store the received replies, a variable to store the received time of the replies and another variable which stores the waiting time for the processing of the replies. The node then starts comparing the sequence numbers of each reply with that of the generated sequence number if the sequence number is much higher than the one contained in the RREQ message then that reply is discarded and hence the black hole attack is mitigated.

2.7 Using FBC Technique

Sengar et al [9] proposed a fuzzy based controller to detect the secure path by nature of association of nodes categorized as good, bad and well known nodes to detect single and cooperative black hole. Since MANET incorporates dynamic topology, the characteristic and the environment keeps on changing as a result the properties of a node also changes with time. The authors have proposed to extend the association based routing using the DSR routing protocol. Every node is mapped to a membership value using the proposed membership function [9]. The authors have assigned three different ranges of values to categorize the nodes. The authors have devised a formula to calculate the trust level of a node. This trust level acts as the parameter to detect a malicious node.

2.8 Using Authentication Terminologies

Khetmall et al [10] presents the use of AODV routing protocol along with addition of some authentication terminologies to detect black hole attack. The terminologies are Authenticated Node (*Authn*) , Authentiacation on path (*Authp*) , Auth Key Packet (*Authkey*) and *Acknowlegement* [10]. If the node has done successful transmission then the status of its *Authn* is marked as True. If the Authentication on node could not be determined then the node moves to the second terminology i.e. Authentication of path, in which other alternatives of trusted route are discovered. *Auth key packet* is used for the authentication of the destination node and *Acknowledgement* is sent by the destination upon successful receiving of the data packet.

2.9 Using Fuzzy Logic Approach

Ramkumar and Urugeswari [11] have proposed fuzzy logic system to detect black hole attack. The authors proposed the incorporation of fuzzy system in each node, they call these nodes as fuzzy nodes. The fuzzy system works in collaboration with AODV routing protocol. The fuzzy system as modeled by the authors in [11] consists of the following four systems.

- *Fuzzy factor withdrawal:* this system extracts the parameters used for analyzing the network traffic to detect a threat.

- *Fuzzy calculation:* this module accepts the analyzed network traffic result and applies the fuzzy rules to calculate the fidelity level [11].
- *Fuzzy confirmation Module:* the Fuzzy confirmation module then compares this values with the set threshold and take the action accordingly.
- *Alarm Packet Generation Module:* finally this module generates the alarm packet with the IP address of the malicious node and alerts the network about it.

This approach is simple and flexible. The additional benefit of fuzzy logic approach is that it can tackle even those problems which do not have complete or appropriate data.

2.10 Using Trust Factor of Node

Suparna et al [12] has proposed a protocol that relies on certain parameters which decide the trust factor of a node and hence helps in selecting the most reliable node towards the destination. The authors state that it is important to trust a node before a packet can be transmitted to/through them. In their work, every node is assigned a *Rank* [12], which is some value greater than '0'. If a packet is dropped by a node and its acknowledgement is not received by the sender, t the rank of the node is reduced by one and if once the rank of a node reaches '0' it is recognized as an attacker. Through simulation the authors have shown the efficient recourse utilization, which helps each node to conserve their power for future use which eventually increases the QoS (Quality of Service) and provides good throughput.

Bar et al [16] proposed a method to exclude black hole attack in MANET. They have obtained a trust value for each node depending upon the packet forwarding ability of the node and a rank was generated based on that trust value. During route discovery, the AODV selects a path in such a way that only the trusted nodes are involved and non-trusted nodes are excluded from the route. Hence, the packet is transmitted through a more trusted path.

2.11 Using Permutation Based ACK

The mechanism proposed by Dave and Dave [13] is an enhancement of the adaptive acknowledgement (AACK) and TWO-ACK. They have proposed AOMSR (Ad-hoc On-demand Multipath Secure Routing) which uses permutation based acknowledgement. The source node is required to store all the paths retrieved to the destination. After finding many routes to the destination, the source node sends different packets via different routes to the same destination. Upon receiving the packets the destination node stores the required entry and sends back a *Permutated Acknowledgement* [13] to the sender. Based on the absence of these acknowledgement packets the black hole attack can be detected.

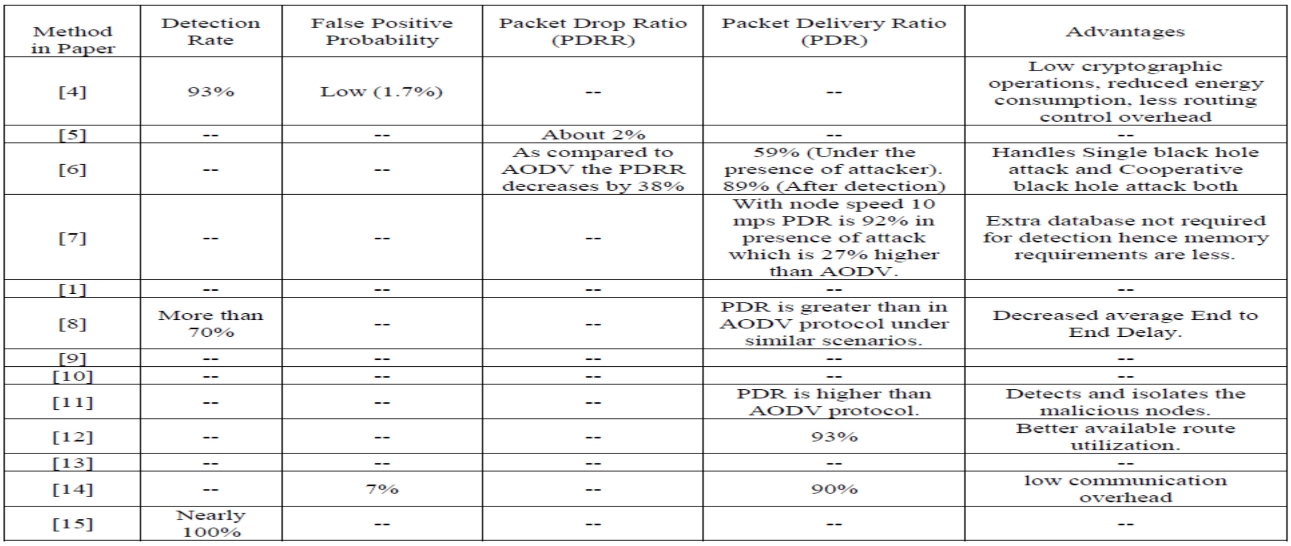
2.12 Using DRI Table and Cross Checking

Sen et al [14] presented a modified AODV routing protocol by introducing data routing information table (DRI) and cross checking. For the route discovery process, the responding node transmits additional two bits of information to the sender node. Each node stores an additional DRI table which has all its neighbors representing each row and two columns namely *from* and *through* which stores value '1' in its entry if the node has sent any packet through the node corresponding to that row or forwarded its packet. All such nodes having a '1' in its through column are marked as *reliable node* [14]. The cross checking method makes use of the reliable node for its operation. In the cross checking method, any intermediate node while responding to the source node, has to send information regarding its next-hop node (NHN) and its DRI entry for that NHN [14]. If the responding node is verified by the NHN then the route is assumed to be secure else the route is insecure.

2.13 Using Destination Sequence Number

Zhang et al [15] have proposed a black hole attack detection method based on the sequence number (SN) in the route reply message. They have employed a control message which informs the source node about the most up-to-date SN. The attacker can deceive the source node about the route to the destination by returning a RREQ message which has a very large SN. An intermediate node sends back a RREP to the source node, at the same time a control message is also sent to the destination node which replies back with the most recent SN. This message is propagated to the source node and hence the attacker can be easily identified on comparing the SN sent by the destination and that produced by the replying node.

A brief summary stating features of the various black hole attack detection methods and protocols discussed and reviewed in the paper is given in figure 1.



Method in Paper	Detection Rate	False Positive Probability	Packet Drop Ratio (PDRR)	Packet Delivery Ratio (PDR)	Advantages
[4]	93%	Low (1.7%)	--	--	Low cryptographic operations, reduced energy consumption, less routing control overhead
[5]	--	--	About 2%	--	--
[6]	--	--	As compared to AODV the PDRR decreases by 38%	59% (Under the presence of attacker). 89% (After detection)	Handles Single black hole attack and Cooperative black hole attack both
[7]	--	--	--	With node speed 10 mps PDR is 92% in presence of attack which is 27% higher than AODV.	Extra database not required for detection hence memory requirements are less.
[1]	--	--	--	--	--
[8]	More than 70%	--	--	PDR is greater than in AODV protocol under similar scenarios.	Decreased average End to End Delay.
[9]	--	--	--	--	--
[10]	--	--	--	--	--
[11]	--	--	--	PDR is higher than AODV protocol.	Detects and isolates the malicious nodes.
[12]	--	--	--	93%	Better available route utilization.
[13]	--	--	--	--	--
[14]	--	7%	--	90%	low communication overhead
[15]	Nearly 100%	--	--	--	--

Fig 1: Features of Various Black Hole Attack Detection Methods

3. CONCLUSION

Various methods and protocols for detecting black hole attack in MANET is discussed and presented in the paper. It is seen that every method/protocol has some issues to be taken care off. Also there is a need to do more research to improve these methods. The paper has highlighted features of the methods reviewed in the paper.

4. REFERENCES

[1] Shraddha Raut and SD Chede, "Detection and Removal of Black Hole in Mobile Adhoc Network", International Journal of Electrical and Electronics Engineering (IJEEE) volume-1 Issue 4, 2012 pp.84-86

[2] Neeraj Arora and N.C. Barwar,"Performance Analysis of Black Hole Attack on different MANET Routing Protocols", International Journal of Computer Science and Information technologies, volume 5(3), 2014, pp 4417-4419.

[3] C.E. Perkins and E.M. Royer, "Ad-hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp 90-100.

[4] Bo Sun, Yong Guan, Jian Chen, Udo W. Pooch, "Detecting Black-hole Attack in Mobile Ad-Hoc Network", 5th European Personal mobile Communications Conference, Glasgow, April 2003 Volume 492, Issue 22-25 pp. 490-495.

[5] Shekhar Tondon and Praneet Saurabh, "A PDRR based detection technique for blackhole attack in MANET", International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, pp 1513-1516

[6] 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", 3rd IEEE International Advanced Computing Conference(IACC), 2013, pp 499-504.

[7] Govind Sharma, Manish Gupta, " Black Hole Detection in MANET Using AODV Routing Protocol", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, January 2012, pp 297-303.

[8] Vipin Khandelwal and Dinesh Goyal, " BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013, pp 1555-1559.

[9] Mamta Sengar, Pawan Prakash Singh, Savita Shiwani, "Detection of Black Hole Attack In MANET Using FBC Technique", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 2, March – April 2013, pp 269-272.

[10] Ms.Chetana Khetmal1, Prof.Shailendra Kelkar2, Mr.Nilesh Bhosale3, "MANET: Black Hole Node Detection in AODV", International Journal of Computational Engineering Research, Vol, 03, Issue, 6, pp 79-85.

[11] J. Ramkumar, R.Murugeswari, " Fuzzy Logic Approach for Detecting Black Hole Attack in Hybrid Wireless Mesh Network", 2014 IEEE International Conference on Innovations in Engineering and Technology (ICIET'14), Volume 3, Special Issue 3, March 2014, pp 877-882.

[12] Suparna Biswas, Tanumoy Nag Sarmistha Neogy, "Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET", Applications and Innovations in Mobile Computing (AIMoC), 2014, pp 157-164.

[13] Dhaval Dave Pranav Dave, "An Effective Black Hole Attack Detection Mechanism using Permutation Based Acknowledgement in MANET," International conference on Advances in Computing, Communications and Informatics(ICACCI), 2014, pp 1690-1696.

[14] J. Sen, S. Koilakonda, and A. Ukil, "A Mechanism for Detection of Cooperative Black hole Attack in Mobile Ad Hoc Networks", In Proceedings of the 2nd International Conference on Intelligent Systems, Modeling and Simulation (ISMS'11), pp. 338-343, Phnom Penh, Cambodia, January 25-27, 2011.

[15] XiaoYang Zhang, Yuji Sekiya and Yasushi Wakahara, "Proposal of a Method to Detect Black Hole Attack in MANET", International symposium on Autonomous Decentralized system (ISADS), 2009, pp 1-6

[16] Bar, R.K, Mandal, J.K, Singh, M.M.**,"**QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack", Elsevier Procedia Technology volume 10,2013, Elsevier DOI: 10.1016/j.protcy.2013.12.392, pp 530-537, 2013.