International Journal of Future Generation Communication and Networking
Vol. 9, No. 12 (2016), pp. 295-304
http://dx.doi.org/10.14257/ijfgcn.2016.9.12.27

A Survey of Black Hole Detection Policies in Mobile Ad Hoc Networks

Kanchan Bala

Department of Computer Science
CT Institute of Technology and Research Maqsudan, Jalandhar
kanchukashyap@gmail.com

Abstract

A mobile ad hoc network (MANET) is defined as a network that has many free nodes that are composed of mobile devices that can arrange themselves in various ways. The important aspect of the MANET is security. In MANET the nodes are connected with the help of its dynamic topology and leave network at arbitrary locations. Ad-hoc On-Demand Distance Vector (AODV) protocol provides dynamic routing between mobile nodes that wish to establish and maintain an ad hoc network. The working of AODV protocol is affected by a particular type of attack called black hole attack.

Keywords*: Mobile adhoc network (MANET), Adhoc on Demand Distance vector (AODV), Route Request (RREQ), Route Reply (RREP)*

1. Introduction

In MANET, a set of mobile hosts with wireless network interfaces form a provisory

Network without the assistance of any fixed or centralized infrastructure. The security implementation is difficult due to absence of any type of open wireless medium and fixed Infrastructure. Each node In MANET acts as a host as well as router that forward packets to the other nodes in network. MANET is assailable to attacks; one of them is Black hole attack.

Figure 1. MANET Network

In Black hole attack, an envious node sends a forged Route REPLY (RREP) packet to the source node that begins the route discovery in order to pretend to be a destination

ISSN: 2233-7857 IJFGCN

node. This attack is launched by advertising a new route with minimum hop count and maximum destination sequence number to the node which initiates the route discovery.

2. Routing Protocols

Now, we are going to explain routing protocols used in MANETs, such as shown in the diagram.

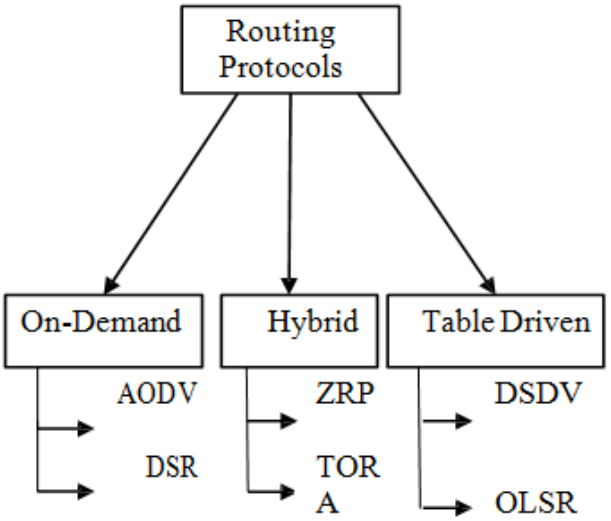

Figure 2. Routing Protocols in MANET

On-demand Routing Protocol

AODV is a routing protocol in MANET that stands for ad hoc On-demand distance vector. It can perform both kind of routing that is unicast ad multicast. It builds the tress which connects the members of multicast group. This routing protocol is scalable. This is named as on demand protocol because it provides the route to destination only if source node needs the route or asks for the route. A route is created between the communicating nodes and there is no fixed existing route.

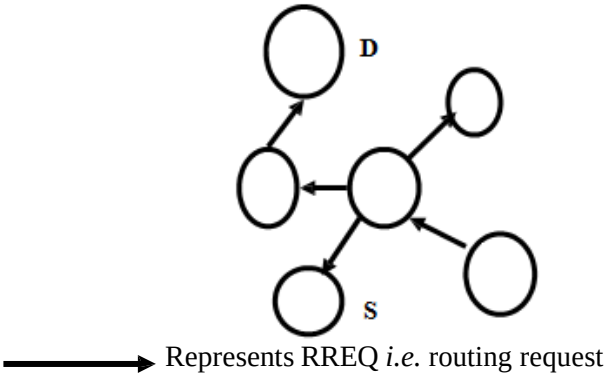

Figure 3. Route in AODV

A node initiates route discovery process when it needs to send packets. There are two types of messages used that are Route Request (RREQ) and Route Reply (RREP). RREQ messages are sent by requesting node to its neighbors who further broadcasts these messages to their neighbors and so on. Destination node or Intermediate node that hasRoute to destination replies to RREQ with RREP. When the intermediate node

replies to the RREQ, then it is called Gratuitous Route Reply. The validity of the route is considered to be valid only if destination sequence number is higher than the previously calculated sequence number. Requesting source node decides the route for the packet transmission from which node it received RREP first.

Table-driven Routing Protocol

The table-driven routing protocol is also known as proactive protocol. During this routing the packets are periodically broadcasted by the mobile nodes to their neighbors. Here every node must manage their routing table that records the adjacent nodes, the number of hops or possible nodes. We can also say, all the nodes have to evaluate their Neighborhoods. Therefore, the drawback of this protocol is that the overhead rises as the network size increases. The advantage of this protocol is that if the malicious attacker joins then network status can be immediately reflected.

Hybrid Routing Protocol

The hybrid routing protocol combines the advantages of On-demand routing and table driven routing to overcome their shortcomings. Hybrid routing protocols are designed as a layered architecture. Initially, table driven routing is applied to gather the unfamiliar routing information. After that On-demand routing is used to maintain the routing information after changing the topology of network.

3. What is Black Hole Attack?

Black hole problem is a matter of worry in ad hoc network. In this problem, an envious node advertise itself as having the shortest path to the node whose packets it wants to intercept by using routing protocol. When malicious reply reaches to the requesting source node before the actual reply, then a forged route is found. This faulty node decides either it should drop the packets to show a denial of service attack or to use its place on the route. This envious node can attack from any side either from inside the network or from outside the network that will be known as external black hole attack and internal black hole attack.

1) EXTERNAL BLACK HOLE ATTACK

External black hole attacks physically lie outside the network and create congestion in network by disrupting the entire network. External attack can also act as internal attack when it takes control of internal envious node and control this node to attack on the other nodes in MANET. The following functions occur in this kind of attack.

- The envious node first searches the route and notes the destination address.
- After that envious node sends a RREP with the noted destination address that is bluffed to an unknown destination address. The lowest value is provided to the hop Count and highest value is provided to the sequence number.
- The envious node sends RREP to its nearest node that belongs to the detected active route.
- RREP received by the nearest node from the envious node will relayed via established route to the source node. The new information that is received through RREP will allow the source node to update its routing table.

2) INTERNAL BLACKHOLE ATTACK

In internal black hole attack envious node lies within the network or we can say in between the routes of source and destination. This node prepared itself as an active

data route element as it presents internally. Now this node can launch attack in the network. Internal attack is more dangerous than the external attack.

4. Types of Black Hole Attack

This attack is of two types such as following:

A) SINGLE BLACK HOLE ATTACK

In this problem a faulty node advertise itself as the shortest route to the destination but it drops the packets instead of transferring them to the next nodes. This attack is represented in figure 1. In this we have given numbers to the nodes as the identifiers. Node 1 will be the source node and node 4 will be the destination node. Node 3 represent the faulty node; it sends false reply to the source node that it has the shortest path to the destination node. The source node mistakenly considers this node as the true route and transfers the packets to it. This node may drop the packet or may consume these packets. This node 3 is black hoe attack and will create problem for the whole network.

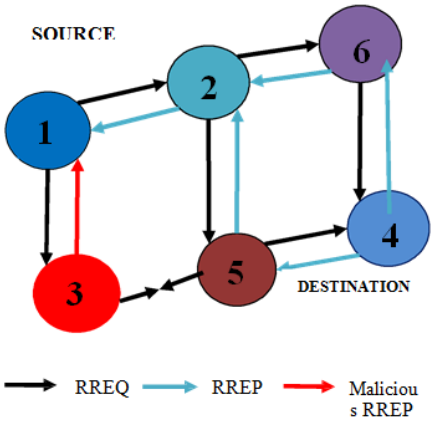

Figure 4. Single Black Hole Attack

B) COLLABORATIVE BLACK HOLE ATTACK

In community oriented dark opening assault number of false hubs teams up with the goal that they can control unique directing data to copy steering data. This kind of attack is represented in figure 5. In this node 3 and node 5 are the faulty nodes that are creating black hole attack.

5. Detections Policies

Detection policies for detecting single black hole attack:

a) Neighborhood based Routing Recovery Policy

This detection policy uses the neighborhood method to detect the black hole attack and to construct accurate route to the destination. This method recognizes the faulty nodes that create single black hole attack in the network. Modify Route Entry control message is send to the destination node to renew its routing path in the recovery protocol. In this policy the detection time is low and high throughput is achieved. The detection is always accurate in this policy. This detection policy becomes fail when faulty nodes collaborate to synthesize.

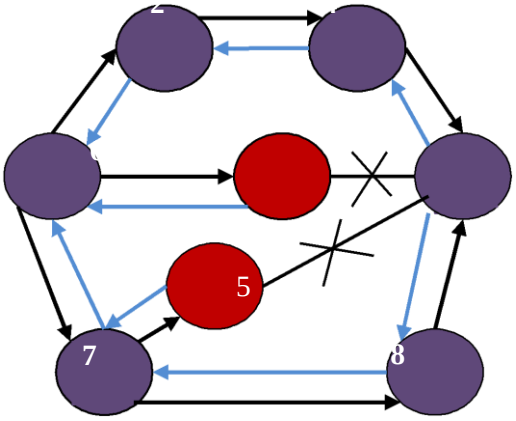

Figure 5. Collaborative Black Hole Attack

b) Duplicate Route Method and Unique Sequence Number policy

Mohammad Al-Shurman *et al*. has proposed two solutions to avoid these black hole attacks. In first solution more than a single path is created from the source node to the destination node. There exist some duplicate paths within the original path, and the authors suppose there are three routes at least. In this, the source node sends a ping packet or a RREQ packet to the destination node. The node which has route to the destination node will reply this request and an acknowledgement is sent by the source node. Now the buffering of the RREP packets is done by the sender until it receives more than two RREP packets, and transfers the buffered packets after getting a safe path. The source node gets the safe path by recognizing the number of hops or nodes and prevents the attack. Second solution uses the idea of unique sequence number. The sequence value is stored; hence it's ever higher than the current sequence number. In this we need to record the values in two other tables that is sequence number for the last packet sent to each node and sequence number of last packet received. These two tables will itself update the values when any packet is sent or received. By checking these two tables, the source node can identify whether there is an envious node present or not. It has been analyzed these two solutions have lesser number of RREQ and RREP messages than AODV. The solution two is better than solution one due to calculation of sequence number.

c) Intrusion Detection Policy based on Anti-black hole mechanism

Ming-Yang Su proposed an Intrusion Detection Policy (IDS) to detect and prevent the black hole attacks, and placed an anti-black hole mechanism (ABM). The two tables that is RQ and SN tables are used to record values in this mechanism. The RQ table always records the RREQ messages within IDS transmission range. The columns of the RQ table are source ID, destination ID, sequence number of source, maximum value of hop count, finish time and ID of the broadcasting node and the columns of the SN table are node ID, status and false values. The SN table is used to record the value of false nodes.

Table 1. Comparison of Single BLACK hole Detection Policies

Detection Schemes	Routing Protocol	Type of attack	Year of publication	Results	faults
Neighborhood d-based and Routing Recovery	AODV	Single Detection	2003	The probability of one attacker can be detected is 93%	Failed when attackers cooperate to forge the fake reply packets
Duplicate Route and Unique Sequence Number policy	AODV	Single Detection	2004	Verify 75% to 98% of the routes	Attackers can listen to the channel and update the tables for last sequence number
Random Two-hop ACK and Bayesian Detection policy	DSR with GloMoSim-based	Cooperative detection	2007	The true positive rate can achieve 100% when existing 2 witness	The proposed scheme is not efficient when value of k is 3
React	DSR	Single Detection	2009	It minimize the communication overhead but enlarges the identification delay	The binary search method is easily expose audit node's information
DPRAODV	AODV	Single Detection	2009	The PDR is improving by 80-85% than AODV when under black hole attack	A little bit higher routing overhead and end-to-end delay than AODV
Next Hop Information Scheme	AODV	Single Detection	2010	The PDR is improving by 40-50% and the number of packets dropped is decreased by 75-80% than AODV	Few additional delay
IDS based on ABM	MAODV with NS-2	Single Detection	2010	The packet loss rate decreases to 11.28% and 14.76%	failed at cooperative black hole attacks

Detection policies for collaborative black hole Attack:

a) DRI Table and Cross Checking Policy

Sanjay Rama swami *et al*. proposed this detection policy that is data routing information (DRI) table and cross checking policy. This method detects the cooperative black holes and modifies the AODV to achieve this methodology. In this a DRI table is managed by each node in which 1 represent the true and 0 represent the false. The working of this policy is as following: The RREQ packets are sent by the source node to the node which replies with RREP. The intermediate node sends the DRI table to the source node. The source node compares its own records and DRI table's records to examine intermediate node's honesty. After getting the entire data source node compares the data of DRI table and its next hop information and detects the malicious route and nodes.

b) Bait DSR (BDSR) based on Hybrid Routing Policy

Po-Chun Tsou *et al*. proposed this policy to detect black hole attack in MANET. In this policy before initiating path discovery the source node sends bait RREQ messages. The address of destination may be non-existing or may be random. The entire RREQ have Smaller life period and the faulty nodes easily detected by the initial phase of the process. The reason behind this is that the bait RREQ becomes capable to attract forged RREP from the malicious node.

c) Hash based Policy

Weichao Wang *et al*. proposed this Hash based policy to prevent the collaborative attacks.

The checked node N is needed in this scheme and it is established by the source node. The sequence number of selected packets sent to the node N by the source node. While sending these packets to the node N, an extra random number is attached at the tail of each packet. The intermediate node combines its own random number R and random number of received packets to calculate its value.

Table 2. Comparison of Collaborative Black Hole Detection Policy

Schemes	Routing protocol	Publication year	Results	Defects
DRI and cross checking	AODV	2003	No simulation results	-
DRI table and cross checking using FERQ and FERP	AODV	2007	A higher throughput performance almost 50% than AODV	5-8% more communication overhead of route request
DCM	AODV	2007	The PDR is now improved from 64.14 to 92.93%, and the detection rate is higher than 98%	A higher control overhead than AODV
Hash based Hashed-based	DSR	2009	No simulation results	-

MAC and Hash-based PRF Scheme	AODV	2009	The PDR becomes higher than 90% when AODV is not accessed	The malicious node is able to forge a fake reply to dodge the detection scheme
BBN and RIP	AODV	2010	No simulation results	-
BDSR	DSR with Qual NET	2011	The PDR of BDSR is always higher than 90%	The overhead is higher than DSR

6. Conclusion

There are many techniques for detecting black hole attack. We have discussed few of them. According to the tables discussed above (table 1 and table 2) the Random two-hop technique is best for detecting single black hole attack and distributed cooperative technique is best for detecting collaborative black hole attack.

7. Future Scope

As we have told in the conclusion that Random two-hop technique is best for detecting single black hole attack and distributed cooperative technique is best for detecting collaborative black hole attack, yet these two have some limitation s also. If we do some more research on these techniques, they would become more efficient.

References

[1] R. Kaur and J. Kalra, "A review paper on blackhole detection and prevention", International journal of advance research in computer science and Software Engineering, **(2014)**, pp. 37-40.
[2] F. H. Tseng, L. D. Chou and H. Chieh, "A survey of blackhole attacks in wireless mobile ad hoc networks", human centric computing and information sciences, **(2011)**.
[3] A. Sharif, M. Elsabrouty and A. Shoukry, "A Novel Taxonomy of Black-hole Attack Detection", IEEE 16th International Conference on Computational Science and Engineering, Alexandria University, Alexandria, Egypt, **(2013)**.
[4] M. A. Shurman and S. M. Yoo, "Black Hole Attack in Mobile Ad Hoc Networks".
[5] J. L. Burbank, P. F. Chimento, B. K. Haberman and W. T. Kasch, "Key Challenges of Military Tactical Networking and theElusive Promise of MANET Technology", IEEE Communication Magazine, vol. 44, no. 11, **(2009)**, pp. 39–45. doi: 10.11.09/COM-M.2006.248156
[6] A. S. Kushwah, K. Khatri and A. Singhal, "A Review on Prevention and detection Techniques for Black Hole Attack in Manet", ISSN: 2319-6327, vol. 2, no. I, **(2013)**, pp. 24-27.
[7] Local data collection Local Detection Cooperative Detection Global Reaction Chanchal et al., International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4, **(2013)**, pp. 820-823 © 2013, IJARCSSE All Rights Reserved Page | 823
[8] H. Weerasinghe and H. Fu, "Preventing, Cooperative black hole attacks in mobile adhoc networks:simulation implementation and evaluation", Future generation communication and networking, vol. 2, **(2007)**, pp. 362- 367.
[9] L. Tamilselven and Sankaranarayanan, "Prevention of Black Hole Attack in MANET" International Conference on wireless Broadband and Ultra Wideband Communications, **(2007)**.
[10] B. Sun, Y. Guan and U. W. Pooch, "Detecting Black Hole Attack in Mobile Adhoc Networks", Paper presented T 5th European Personal Mobile Communication Conference, **(2003)**.
[11] F. H. Tseng, L. Chou and H. C. Chao, "A survey of black hole attack in wireless mobile adhoc networks", springer journal, **(2011)**.