Indian Journal of Science and Technology, Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/107994, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Averting Techniques of Black-Hole Attack –A Survey

P. Pavithra*

School of Computing, SASTRA University, Thanjavur, Tamil Nadu, India; pavithrapandian18@gmail.com

Abstract

Objectives: To identify the black-hole attack. The Ad hoc is a self-configuring network it can be configured at anytime and anywhere without pre-defined infrastructure due to unique characteristics. **Methods:** Black hole is a traffic relaying attack in network layer. The intermediate node involves in forwarding a message to the destination in Multi-hop ad hoc network. These nodes will launch black hole attack to conserve its resource or to perform attacks that reduce the network performance. This attack is carried by the interposed node instead of forwarding the packets this node will carry the action of dropping packets. **Findings:** We can avoid this attack by using cryptography methods like symmetric encryption, asymmetric encryption and non-cryptography methods like IDS (Intrusion Detection System). This attack can also be avoided by clustering method where we can also reduce the cost. **Applications:** Many researchers have been carried out for the detection of black hole attack. In this paper we are going to discuss different techniques given for averting the black-hole attack.

Keywords: Adhoc Network, Black Hole, Intrusion Detection System (IDS), RREP, RREQ

1. Introduction

The ad-hoc network is a network launched without any pre-defined infrastructure so that it can be configured at any point of time. The ad-hoc network is established for a short period. The node in ad-hoc network is dynamic so the ad-hoc protocols are configured such that it can adjust to any traffic and environment. Ad-hoc network is formed using multiple nodes. Since ad-hoc is made up of multiple nodes it possess many characteristics like less bandwidth, low battery, short life span, low computational power and more.

The ad-hoc network support two topologies Heterogeneous and Homogeneous .In heterogeneous topology the node connected the network have different capabilities and in homogenous topology the node connected to the have same capabilities. In an add-hoc network each and every node will act as both router and host. Each host in the network i.e., node will support peer-to-peer communications (node will directly communicate to its destination) and peer-to-remote communication (node will communicate to its destination through interposed node).

In adhoc help of the interposed node are needed to hand over the packets to destination. If the node is within the coverage area they can communicate directly if they are not in the coverage area the interposed node will be considered as a router and it will forward the packets to the destination. Since In multi hop wireless ad-hoc interposed node are needed to hand over the packets to destination it can launch packet dropping attack to conserve its resource or to perform denial-of-service.

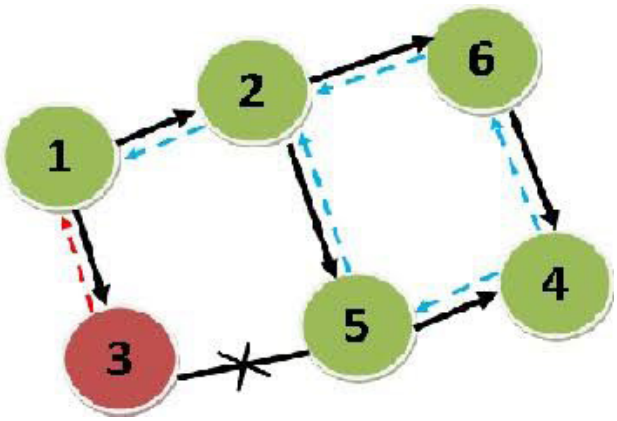

Figure 1. Simple black-hole attack.

*Author for correspondence

Wireless ad hoc network is formed using multiple nodes. Since ad hoc is made up of multiple nodes it possess many characteristics like less bandwidth, battery, lifespan and computational power because of these properties this network is sensitive to many attacks like DoS attack, misbehaving. The consequences of this attack are decadence in network communications, impassable nodes, and possible routing loops. We can overcome these attacks by using cryptography methods like symmetric encryption, asymmetric encryption and non-cryptography methods like IDS (Intrusion Detection System).

1.1 Black-hole attack

Black-hole attack is a passive attack it won't modify the message and also an type of denial-of-service attack. To conserve its resource or to perform attack the black-hole attack is performed so that it reduces the network performance. The black-hole nodes assure that it has a very new and small route to destination and once the malicious path is selected that node drop the packet instead of forwarding the packet it will affect the network performance. This attack can be done particularly (Specified destination packets are discarded, a randomly selected fragments of the packets are dropped or every i packets is dropped) or each and every packet is dropped, and may have the effect of making decadence communications in the network or the destination node impassable. This attack is performed either in simple or cooperative manner.

1.1.1 Simple Black-Hole Attack

The simple black hole[1] is shown in Figure 1.This attack is carried out by an individual node in a network. Routing protocol is violated and attack is launched by a single i.e. individual node. In the diagram let the node 4 is the black-hole node. That black hole node will send a fake response to the request, when the malicious path is selected as a route that node will start dropping the packets instead of forwarding them.

1.1.2 Cooperative Black-Hole Attack

In the network if more than one node performs a attack cooperatively then that black-hole attack it is known as cooperative black-hole attack. It is shown in the Figure 2. And the node which performs this attack is said to be black-hole node. In the diagram both the node 3 and 5 will combine with each other and perform the attack.

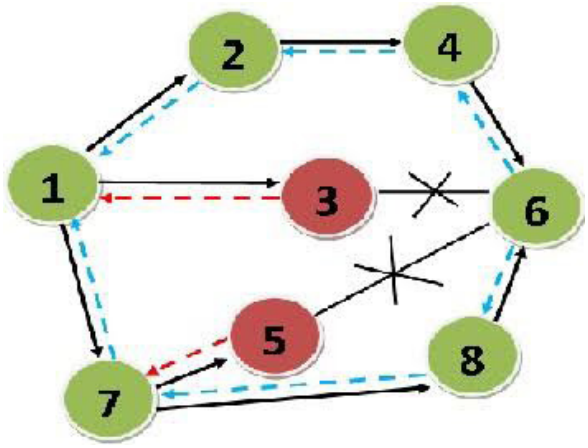

Figure 2. Cooperative black-hole attack.

2. Detection techniques

In the table 1 method to avoid black hole and its drawback is explained.

In[1] has modified the routing protocol.Using this modified routing protocol they has identify the black-hole node that is present in the network. The intermediate node is cross checked through the another route i.e., when a interposed node tell that it has a route that interposed node is verified through another way this done to audit whether it has a way to destination are not. If it is a malicious node then intimation sent to all the node. The proposed method can identify the black-hole node efficiently but the main drawback of this method is the cooprative black hole attack cannot be identified i.e this method fails when two or more cooprate with each other to conduct attack.

In[2] has used the concept of repeated next hop node information to identify the black-hole node.Message is sent once to node which send reply and wait for sometime to verify that node.Next hop infromation is also collected from the node.And wait for the RREP from all the nodes are collected by the source until timer expire. After that the data is sent through the repeated next hop node .

In[3] used a concept of Merkle tree concept i.e., the nodes are consider in the tree like structure then the verification is done to identify the black-hole attack.To identify the black-hole one way hash function is used.The one way hash function is the secure way of communication.

In[4] has used a Hashed message authentication code (HMAC). HMAC is used for message verification ,sender

Table 1. Different detection techniques

S. No	References	Year	Method	Drawbacks
1	1	2002	Modified routing security protocol	More false positive
2	2	2007	Repeated Next Hop Information	Computation and routing overhead is more
3	3	2010	Used principle of Merkle tree	More traffic
4	4	2011	Used Hashed message authentication code (HMAC)	RREP message can't be verified
5	5	2012	Intrusion detection and response protocol for MANET is used	False positive is more
6	6	2012	CCHF	Delay and complex computation
7	7	2013	Judgement Process	Prediction can be wrong
8	8	2013	Used IDS	Failed at cooperative black hole attack
9	9	2013	Triangular encryption	Communication overhead
10	10	2013	Asymmetric encryption	Computation overhead
11	11	2013	Identity based key management	Data packets are exposed
12	12	2013	Monitored by neighbour	False Negative is possible
13	13	2014	End-to-end acknowledgement	Communication overhead
14	14	2014	Clustering	Communication complexity
15	15	2014	Nested message authentication for secure AODV routing	Computation overhead
16	16	2015	Energy based clustering	Communication complexity
17	17	2015	Anamaly based IDS	More energy is needed

authorization, as well as intermediate nodes authentication. Between source and destination secret key is shared and each node holds HMAC. Using this hashed message authentication we can find the Black-hole node and avoid this aattack.

In[5] proposed an intrusion detection system to identify the black-hole node.IDS will monitor the node regularly and based on their activites the it identify the malicious one.In this paper then intrusion detection and response protocol is used to identify the black hole attack. IPS is a intrusion prevention system that blocks the misbehaving node and send information to the source node.

In[6] has used Symmetric cryptography with cyclic chain hash function (CCHF) to identify the black hole attack.Cryptography is the process of converting the message into an unreadable format. The new method is proposed for generation of ID key for authentication of node because of this method black-hole node can be identified.The drawback of this approach is Cooperative cannot be identified.

In[7] Used the activities of nodes in network to black hole attack is identified. The judgement process is first initiated by the first reciever of the RREP packet , this node will monitor the neighbours activities and make the decision. The decision is made by following rules.

- Rule 1 : If delivery of data is more then that node is honest.
- Rule 2 : If data packets are not sent then the node is misbehaving.

With the help of ablove two rules the black-hole node is identified.

In[8] have used the Intrusion detection system (IDS) to detect the black hole attack.IDS will monitor the node activity and identify the black-hole. Each and every

system in the network contains IDS that monitors neighbours activity, Network and system audit data is used to detect the malicious node then the report is sent to the security management. But false positive is more i.e., it fails to identify the black-hole when mobility increases.

Black hole attack is identified using triangular encryption method[9]. When destination recieves the RREQ it encrypts the text with pre agreed partition and key, this encrypted data is sent along with the RREP . Black hole node will not have this chiper text.

In[10] proposed Asymmetric cryptography method and is used with RSA algorithm for hop count encryption. When source wants to communicate, destination node sends it public key to the source node. It encrypts the message with public key which can be only decrypt by destination node.

In[11] has used Identity based key management. It is a combination of ID based cryptography and threshold cryptography used to authenticate all routing message. Since malicious node is unaware of security it couldn't enter into the network.

In[12] proposed Real time monitoring to identify the black hole node. The neighbor of RREP generator listen to the packet sent recieved by the RREP generator.

In[13] proposed end-to-end acknowledgment. Each and every node who recieve an RREQ has to send an acknowledgement to the source node. But communication overhead is more in the method.

In[14] has used a clustering concept. In this, entire cluster is divided into many clusters and one node is elected as a cluster head. That cluster head will check the cluster member by getting an acknoweldgement. If acknowledgement is not recieved then that node is marked as a malicious and it is dropped . But the drawback in this method is communication overhead.

In[15] has used Nested message authentication for secure AODV routing i.e., Each node consists of table. Group of similar shared keys are stored in that table and hop count value is verified to elect key, which make it difficult for intruder to exploit the network.

In[16] has used cluster. The cluster is formed based on their energy. Cluster head will act as a check in and check point in the network for the data flow.

In[17] used IDS for detection of black-hole node. Anomaly based IDS is used to identify the black hole attack. This IDS is based on the windowing method to analyse selected cross layer features. This method consume more energy.

In[18] author used a group key to identify the black hole attack. This key is generated using the Diffie-Hellman (DH) method.

3. Conclusion

This paper survey provides current detection and prevention techniques of black hole. In Ad hoc network, the interposed nodes are used for communication and these nodes will launch black hole attack to conserve its resource or to perform attack that reduce the network performance. Many detection and prevention techniques have been discussed above in that they have used different methods like cryptography, IDS and clustering concept to find the black hole attack. But these methods have some disadvantages as we discussed earlier.

4. References

1. Deng H, Li W, Agrawal DP. Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine. 2002; 52(6):227–33.
2. Tamilselvan L, Sankaranarayanan V. Prevention of Blackhole Attack in MANET, IEEE. 2007; 21 pp.
3. Baadache A, Belmehdi A. Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks. International Journal of Computer Science and Information Security. 2010; 7(1):10–6.
4. Sachan P, Khilar PM. Securing AODV Routing Protocol in MANET based on Cryptographic Authentication Mechanism. International Journal of Network Security and Its Applications. 2011; 3(5):229.
5. Maheshwar K, Singh D. Black Hole Effect Analysis and Prevention through IDS in MANET Environment. European Journal of Applied Engineering and Scientific Research. 2012; 1(4):84–90.
6. Singh S, Sharma S, Sahu S. Secure AODV using Symmetric Key Cryptography with Cyclic Chain Hash Function. International Journal of Computer Applications. 2012; 47(18):34–9.
7. Dangore MY, Sambare SS. Detecting And Overcoming Blackhole Attack In Aodv Protocol. International Conference on Cloud and Ubiquitous Computing and Emerging Technologies. 2013; 77–82.
8. Kaur NS, Arora SK. Analysis of Black Hole Effect and Prevention through IDS in MANET. American Journal of Engineering Research (AJER). 2103; 2(10):214–20.
9. Chatterjee N, Mandal JK. Detection of Blackhole Behaviour using Triangular Encryption in NS2. 1 st International

Conference on Computational Intelligence: Modeling Techniques and Applications. 2013; 10:524–29.
10. Kumar SBM, Benni NKS. Cryptographic Approach to Overcome Black Hole Attack in MANETs. International Journal of Innovations in Engineering and Technology. 2013; 2(3):86–92.
11. Gajera M, Sowmya KS. Prevention of Black Hole Attack in Secure Routing Protocol. International Journal of Science and Research. 2013; 2(6):221–24.
12. Kshirsagar D, Patil A. Blackhole Attack Detection and Prevention by Real Time Monitoring, IEEE. 2013; 1–5.
13. Baadache A, Belmehdi A. Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. Computer Network. 2014; 73:173–84.
14. Singh G, Singh G. Detection and Prevention Of Black Hole using Clustering In MANET using Ns2. International Journal of Engineering and Computer Science. 2014; 3(8):7420–42.
15. Arya KV, Rajput SS. Securing AODV Routing Protocol in MANET using NMAC with HBKS Technique. International Conference on Signal Processing and Integrated Networks. 2014; 281–85.
16. Madhura SD, Ramesh B. Detection of Black Hole for Improving Efficiency of MANET using Energy-based Clustering. International Journal of Engineering Research and Technology. 2015; 4(10):3.
17. Casado LS, Fernandez GM, Teodoro PG, Carrion RM. A model of data forwarding in MANETs for lightweight detection of malicious packet dropping. Computer Network. 2015; 87:44–58.
18. Kumar KV, Somasundaram K. An Effective CBHDAP Protocol for Black Hole Attack Detection in Manet. Indian Journal of Science and Technology. 2016; 9(36):1–11.