Detection of Black Hole Attack in MANET: A Review

Sweta Tarale
Department of Computer Science and Engineering, Shri
Shankaracharya Technical Campus, Bhilai , India
e-mail:swetatarale2012@gmail.com

Dr.Abha Choubey
Department of Computer Science and Engineering, Shri
Shankaracharya Technical Campus, Bhilai , India
e-mail:abha.is.shukla@gmail.com

Abstract- Mobile ad-hoc networks are a collection of mobile hosts that communicate with each other without any infrastructure. Security is an essential requirement in mobile ad-hoc networks to provides protected communication between mobile nodes. MANET are vulnerable to various types of attacks .One of main active attacks is black hole attack, it is a denial of service attack and it drops entire incoming packets between one source to destination. In this paper we studied the details about black hole attack, and techniques for detection and prevention of black hole attack.

Keywords*-Mobile ad hoc network(MANET),AODV,Black hole attack,Routing protocol.*

*****

I. INTRODUCTION

Mobile ad hoc network is one kind of new wireless network structure. In ad hoc network all nodes are movable and the topology of the network is changing dynamically[1]. MANET can be used to enable next generation battlefield applications. MANETs have some special characteristics features such as unreliable wireless media (links) used for communication between hosts, constantly changing network topologies and memberships, battery, lifetime, and computation power of nodes etc [2]. One of the most widely used routing protocol in MANETs is the ad hoc on-demand distance vector (AODV) routing protocol. Ad-hoc on-demand vector routing is an on-demand routing protocol which confluence of DSDV and DSR .In AODV Routes are established on demand and destination sequence numbers are used to find the latest route to the destination. In this paper a survey of various security mechanisms that have been proposed is presented.

II. RELATED WORK

Researchers have proposed various techniques for detection and prevention of Black hole attack in mobile ad hoc network.

In[3] proposed a solution which is based on cluster organization of network. In this scheme they maintain a history table which contain send packets, received packets, and dropped ratio which is calculated by using received packets/send packets for every node, but no simulation or performance evaluation have been done.

[2] introduces the use of Data Routing Information (DRI) to keep track of past routing experience among mobiles nodes in the network and cross checking of RREP messages from the intermediate nodes. The drawback of this technique is that mobile nodes have to maintain an extra database of past routing experience.

In[4] defines how implement Black hole attack in ad hoc on demand distance vector protocol.

[5] proposed new trust management frame work(TMF),which calculates a node's trust value based on observations from neighbor nodes by using Grey theory and fuzzy logic sets. The TMF chooses multiple rather than a single parameter to obtain trust value. The proposed frame work can do is not only detecting abnormal trust behavior but also discovering parameter for forming trust values.

[6] In this paper, a defense mechanism is presented against a coordinated attack by multiple black hole nodes in a MANET. The simulation carried out on the proposed scheme has produced results that demonstrate the effectiveness of the mechanism in detection of the attack while maintaining a reasonable level of throughput in the network.

In[7] proposed mechanism using a quantitative method to detect intrusion in MANETS with mobile nodes. This method is a behavioral anomaly based system, which makes it dynamic, scalable, configurable and robust. Finally, verify method by running ns2 simulations with mobile nodes using Ad-hoc on- demand Distance Vector (AODV) routing. It is observed that the malicious node detection rate is very good, and the false positive detection rate is low.

[1] proposed path based method to detect black hole attack, and adaptive algorithm to enhance the detection performance by using detection algorithm, it is based on path based scheme that is a node does not watch every node in the neighbor, but only observes the next hop in current route path.

In [8] the author discuss a protocol DPRAODV and the ALARM used in DPRAODV in this scheme the RREP sequence number is extra checked whether higher than the threshold value or not, if the value of RREP sequence number is higher than the threshold value, the sender is referenced as an attacker and updated it to black list. The ALARM is sent to its neighbor who includes the black list, thus the RREP from the malicious node is blocked but is not processed.

III. ATTACKS IN MANET

We have categorized the presently existing attacks into two broad categories: DATA traffic attacks and CONTROL traffic attacks. This classification is based on their common characteristics and attack goals.

DATA traffic attack:

- Black-Hole
- Cooperative Black-Hole
- Grey Hole
- Jellyfish

CONTROL traffic attack:

- HELLO Flood
- Bogus Registration
- Man in Middle
- Rushing Attack
-

A.Black hole attack :

In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting components of that network, then it effectively separates the network into two disconnected components.

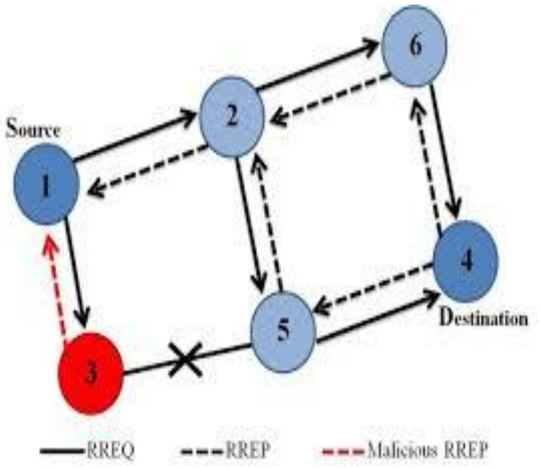

Fig. 1. Black hole attack

B. Cooperative Black Hole Attack:

This attack is similar to Black-Hole attack, but more than one malicious node tries to disrupt the network simultaneously. It is one of the most severe DATA traffic attack and can totally disrupt the operation of an ad hoc network. Mostly the only solution becomes finding alternating route to the destination, if at all exists. According to the original AODV protocol, when source node S wants to communicate with the destination node D, the source node S broadcasts the route request (RREQ) packet. The neighboring active nodes update their routing table with an entry for the source node S, and check if it is the destination node or has a fresh enough route to the destination node. If not, the intermediate node updates the RREQ (increasing the hop count) and floods the network with the RREQ to the destination node D until it reaches node D or any other intermediate node which has a fresh enough route to D, as depicted by example in Figure 1. The destination node D or the intermediate node with a fresh enough route to D, initiates a route response (RREP) in the reverse direction, as depicted in Figure 3. Node S starts sending data packets to the neighboring node which responded first, and discards the other responses. This works fine when the network has no malicious nodes.

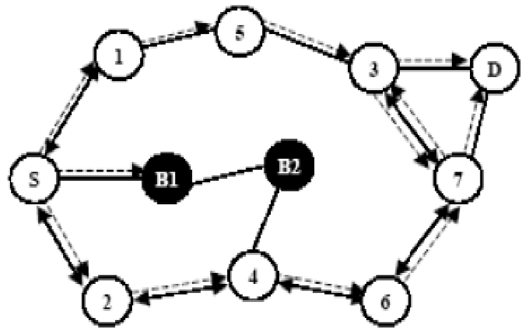

Fig.2. Network flooding by RREQ messages

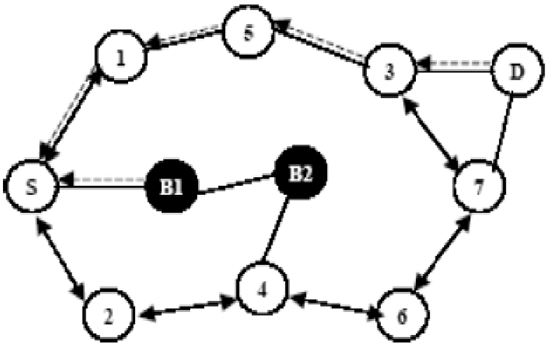

Fig.3. Propagation of RREP messages

IV. CONCLUSION

In this paper, we studied the information about mobile ad hoc network, and black hole attack in MANET. This paper also analyzes different mechanism for detection of black hole attack in MANET.

ACKNOWLEDGMENT

We would like to show our gratitude to the Prof. Samta Gajbhiye, Head of Department of CSE,SSTC for manuscript publishing.

REFERENCES

[1] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, “An adaptive approach to detecting black and gray hole attack in ad hoc network,24th IEEE conference on Advanced Information Networking and Applications,2010.

[2]] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, “A mechanism for detection of cooperative black hole attack in MANET, second IEEE international conference on Intelligent System, Modelling and Simulation,2011.

[3] Shirsty Chandel, Ashish Tiwari, “A weighted clustering algorithm for improving MANET security”, International Journal of Computer Science and Information Technology research,2014.

[4] Monika Roopak, Prof. BVR Reddy, “Black hole attack implementation in AODV routing protocol, International Journal of Sceintific and Engineering Research,2013.

[5] Ji Guo, Alan Marshall, Bosheng Zhou, “A new trust management framework for detecting malicious and selfish behaviour for MANET,International Joint Conference of IEEE,2011.

[6] Sanjay Ramaswamy, Huirong Fu, Monalar Sreekantaradhya, John Dixon and Kendall Nygard, “Prevention of cooperative black hole attack in wireless ad hoc network, IACC.

[7] Suman S Chandrakar, Brajeshpatel, Amit Kumar Chandanan“Detection of suspected nodes in MANET” ACEEE International Journal on Network Security 3, 1 (2012) 6 ACEEE Int. J. on Network Security ,Vol. 03, No. 01, Jan 2012.

[8] Payal N.Raj, Prashant B. Swadas, “DPRAODV: A dynamic learning system against black hole attack in AODV based MANET,International Journal of Computer Science Issues,2009.