International Journal of Engineering Research in Computer Science and Engineering Engineering (IJERCSE) Vol 2, Issue 3, March 2015

Detection of DOS Attacks through Evidence Collection using Dempster-Shafer Theory

[1]Shradha S. Ippakayal,[2]Geetanjali S. Dhaygude,[3]Vinaya P. Kalyanshetty,[4]Prof. M.N.Ingole
[1][2][3][4]Department of Computer Engineering,JSPM's Rajarshi Shahu College Engineering
Pune, India
[1]shradhaippakayal@gmail.com,[2]geetadhaygude25@gmail.com,[3]vinaya231994@gmail.com,
[4]meghna.ingole1983@gmail.com

Abstract **MANETs has been experiencing exponential growth in the past decade. Due to their vulnerability to various attack makes extremely prominent for its distributed and independent nature. Among these various DOS attacks black hole, grey hole, and co-operative black hole attack may collapse the network, and this may become a major threat in MANETs. Here we are using Dempster-Shafer evidence based theory to collect various evidences for various nodes in the network against black hole and grey hole attack. For detecting malicious node we used Direct Trust Value (DTV) to detect a single black hole attack. DTV is calculated for each node that exists in the network and then that value is compared against predetermined threshold, if the calculated value is less then predetermined threshold then the node is malicious node.**

Key words- **Mobile Ad-hoc network, grey hole attack, Black hole attack, Packet forwarding.**

I. INTRODUCTION

Mobile ad-hoc network is a type of ad-hoc network that can change locations and configure itself on the fly. MANET are kind of wireless ad-hoc network that actually has a routable networking environment on top of link layer ad-hoc layer. It consists of peer-to-peer self forming, self healing network in contrast to a mesh network has a central controller. MANET does not depend on preexisting infrastructure. Security problems in MANET mainly arise due to its unique characteristics such as dynamic network topology, limited bandwidth and limited battery power. Cryptography method failed
to figure out compromised nodes or legitimated ones with malicious actions. There are mainly two types of attack active attack and passive attack, passive attacks are attacks which attempts to make use of information from system but does not affect system resources, passive attack includes passive eavesdropping, Sybil attack, Denial of service attack, worm hole attacks. Active attacks are the attacks which attempts to alter the system resources by affecting their operations, they include man-in-middle attack, botnet attack, SYN flood attack etc.
Black hole attack and grey hole attack are the types of DOS attacks, black hole attack damage the normal communication in large area network by dropping the packets completely, grey hole attacks partially send or drop

the data and some time act as honest node, grey hole attacks are difficult to detect, since the sender cannot recognize the malicious node in the network because it sends the acknowledgment to the previous node that the packet is forwarded to the next node.
D-S enables the combination of evidence generated from multiple sensors, e.g. basic detection elements. Each sensor -monitors, detects and reports its own perspective (belief) of the observed cyber and/or physical attributes. The beliefs of several sensors are then combined (fused) in order to provide a unified view of the system state. Sensors act as thin autonomous agents which collaborate by sharing their beliefs about the observed attributes. From our perspective, the cyberphysical system is seen as having a stochastic behavior without assuming any underlying functional model. Moreover, based on the proposed architecture we implement a new cyber-physical anomaly detection system.

I. RELATED WORK

A. Black Hole attack

Black Hole attack is a type of DOS attack which comes under active attack. It is also called as packet drop attack. Black hole attack is the most

All Rights Reserved © 2015 IJERCSE

frequent attack happening in the network which stops the forwarding of data packets. Black hole attack swallows all the data, in this attack the attackers tries to collect most of the data from the network and then drop it. In black hole attack malicious node send a fake routing information that it has finest route and as result all the data packets are attracted towards that fake route and then this fake node drops all the packets and deny the data forwarding to the destination.

There are various routing protocols implemented in MANET, we are focusing on the Reactive protocol. Reactive protocol contains Ad-hoc on demand distance vector routing protocol (AODV).

1. Black hole in AODV

The senders send the fake RREP(route reply) to the source node claiming that it has the fresh and smallest route to the destination node , the source sends the data through the fake node and that fake node drops the data packet.

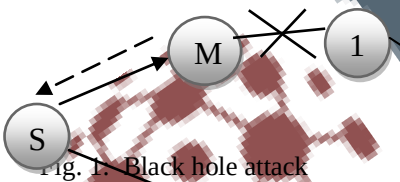

Fig. 1: Black hole attack

S: Source node D: Destination node
M: Malicious node

Indirect route
Route request message
Route reply message
Direct route

B. Grey hole attack

Grey hole attack is type of DOS attack. in this the node behave as a honest node during the route discovery process and then silently drops packet. The data packets are been partially dropped by the node. Grey hole attack consist of two phases, in the first phase the malicious node exploit the AODV protocol to introduce itself as it has a valid route to the destination. The intension of this node is of intercepting the packet even though the route is superious. In second phase this node drops the intercepted packet with the certain probability.

The grey hole attack is more difficult ti detect then black hole attack, where the malicious node drops the received data packets with certain amount.

1. Grey hole attack in AODV

Every node maintains a routing table that stores the next hope information of each node. In the routing table there exists the route and if the route does not exists the node initiates the route discovery process by broadcasting RREQ message to its neighbors, then the neighbors sends the route reply message back to the source node.

C. Co-operative Black Hole Attack

In this source node forwards the packet to the next node, then this node sends the acknowledgment to the source node that data has been forwarded to the next node but it partially sends the data packets to the next node. Then the next node totally drops the data and denies forwarding the data packets to the destination.

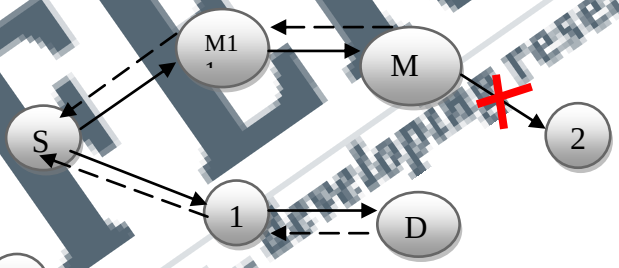

Fig: 2 Co-operative black hole attack

Route request message
Route reply message
Direct route

II. Proposed system

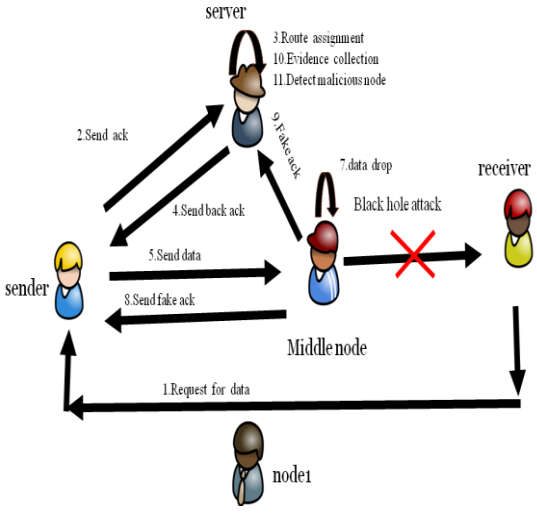

Fig 3: system architecture

All Rights Reserved © 2015 IJERCSE

The proposed system works as follows

1. Network module: this model is used for adding a new node in the network.

2. Data communication
   - 2.1 Request generation
   - 2.2 Channel assignment
   - 2.3 Data transfer initialization

3. Evidence collection using dempster Shafer theory
   In this module the evidences are created for each node.

4. Intrusion detection system
   It monitors every node's activity in the network.

5. Prevention
   After detecting malicious node the system will change the communication channel, so that malicious node get removed.

III. IMPLEMENTATION

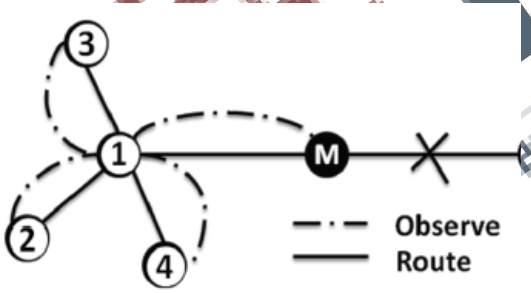

Fig: Neighbor node observation model

The watchdog mechanism is used in neighbor observation model for calculating DTV of each node

Dempster shafer theory

This theory can be interpreted as a generalization of probability theory where probabilities are assigned to sets as oppose to mutually exclusive singletons. The evidence is associated with only one possible event, but in DST evidences can be associated with multiple events, for e.g, set of events. DST model collapse to the traditional probabilistic formulation. Dempster-Shafer Theory (DST) is a mathematical theory of evidence. There are three important functions in the dempster shafer evidence theory:

-The basic probability assignment function (bpa or m).

-The belief function(Bel).

-The Plausibility function(Pl)

- The basic probability assignment function(bpa or m).

$$m:P(X) \quad [0,1]$$

- The belief function (Bel)

$$Bel(A) = \sum_{B|B\subseteq A} m(B)$$

- The plausibility function(Pl)

$$Pl(A) \sum_{B|B\cap A = \emptyset} m(B)$$

CONCLUSION:

Todays biggest challenge is security of MANET's. We focus on AODV protocol and describe black hole and grey hole attack in MANET. DTV is used to detect the black hole attack. evidences of each node in the network. With the help of evidences we detect the malicious node in the network and then change the communication path for data transmission. For detecting co-operative black hole attack ITV is used.

REFERENCES

[1] Steven Abney. Dependency grammars and context-free grammars. manuscript. Presented at meeting of Linguistic Society of America, Jan 1995.

[2] Y. Bar-Hillel, M. Perles, and E. Shamir. On formal properties of simple phrase structure grammars. In Y. Bar-Hillel, editor, Language and Information: Selected Essays on their Theory and Application, chapter 9, pages 116{150. Addison-Wesley, Reading, MA, 1964.

[3]Eliminating co-operative black hole and gray hole attacks using modified EDRI table in MANET, vani A.hiremani,Manisha Madhukar Jadhav,2013

[4] Detection and removal of cooperative black hole and gray hole attack in Mobile Ad hoc Networks,Vishnu K,Amos J Paul,2010

All Rights Reserved © 2015 IJERCSE