International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
*ISSN (Online)*2349-6967 *Volume 2 , Issue 1(Jan-Feb 2015), PP1-5*

Evidence Based Detection of Dos Attack in MANETs

Geetanjali Dhaygude[1], Shradha Ippakayal[2], Vinaya Kalyanshetty[3]
Mrs. M. P. Lokhande[4]
[1 2 3 4] *(Computer, JSPMs RajarshiShahu College of Engineering, India)*
[2]

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 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. 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.[1] 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. Another approach for detecting malicious node to identify [1] co-operative black attack and grey hole attack we are using Indirect Trust Value.

Keywords- 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. MANET are 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, 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 battery power. Cryptography[1] 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, 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. In the pastfew years we have witnessed a rapid increase in the use of Information and Communication Technologies (ICT) within Networked Critical Infrastructures (NCIs), e.g., power plants, water plants and energy smart grids. As a result, it has been possible to implement more efficient and flexible installations as well as new services and features such as remote monitoring and maintenance, energy markets. Although the advantages of this trend are unquestionable, the shift from a completely isolatedenvironment, to a system of systems integration with existing architecture, e.g., the Internet, has lead to the exposure of NCIs to significant threats.

Cyber-physical attacks exploit the cyber and physical dimensions of NCIs and can have serious consequences on their normal operation. Stuxnet, the first malware specifically designed to attack the control hardware of NCIs, was a clear demonstration in this sense and showed a new level of sophistication in malware development. Stuxnetincreased many questions, but highlighted the lack of an efficient approach to detect complex cyber-physical attacks on NCIs. Unfortunately, as stated in the peculiarities of NCIs can render traditional ICT security techniques ineffective when faced with cyber-physical attacks. Therefore, this paper alleviates the aforementioned issues by proposing a novel approach for detecting cyber-physical anomalies in NCIs using the concept of and Dempster-Shafers Theory of Evidence. Dempster- Shafersenables the combination of evidence generated from multiple sensors. Each sensor -monitors, detects and reports its own perspective (belief) ofthe 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. The attempt to infer the unknown state of the system is based on knowledge reported by sensors, that have been own based on totally different criteria. Possible sources of information are signature-based IDS, custom DDoS detection programs, control hardware (e.g. Programmable Logical Controllers PLCs) or physical sensors. The novelty of our approach is that it combines reports of various cyber and physical sensors. Moreover, based on the proposed architecture we implement a new cyber-physical anomaly detection system.

1.Record extraction,
2.Attribute alignment and,
3.Attribute labelling.

II. RELATED WORK

2.1. 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 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).

2.1.1. 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.

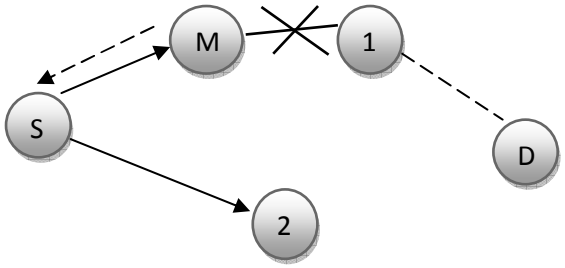


Fig. 1. Black Hole Attack

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

Indirect route

Route request message

Route reply message

Direct route

2.2. 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 to detect then black hole attack.

2.2.1. 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 is 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.

2.3. Co-operative Black Hole Attack

In this source node forwards the packet to the next neighbor 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.

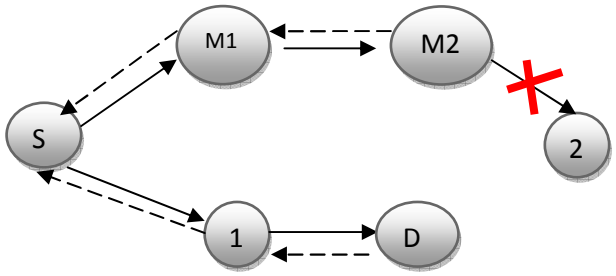


Fig. 2 . Co-Operative Black Hole Attack

III. PROPOSED SYSTEM

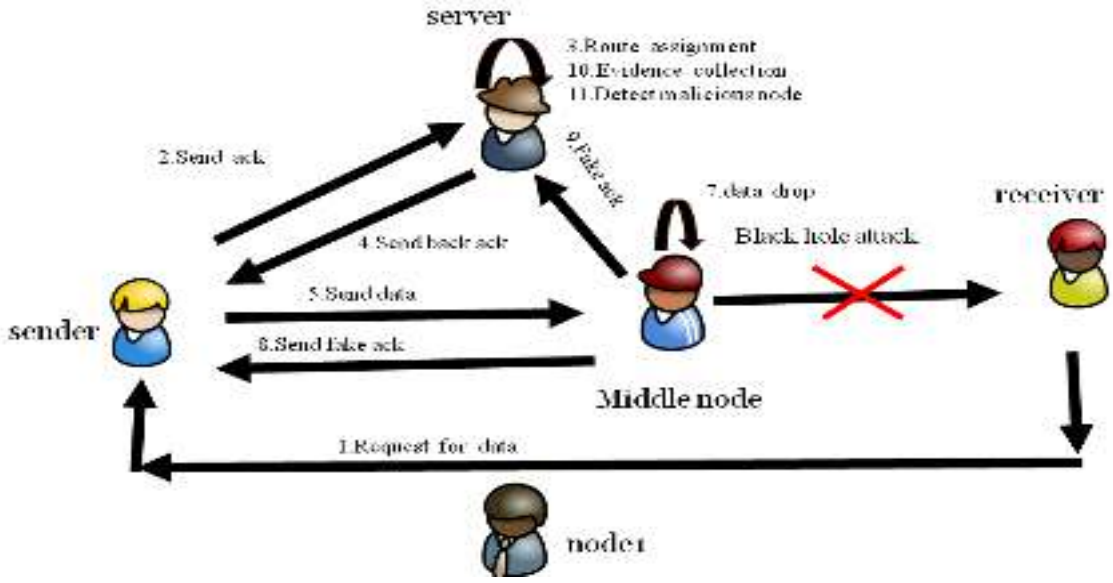


Fig.3: System Architecture

The proposed system works as follows:

3.1. Network module: This model is used for adding a new node in the network.

3.2. Data communication
They are divided into three categories
Request generation
Channel assignment
Data transfer initialization

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

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

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

4. IMPLEMENTATION

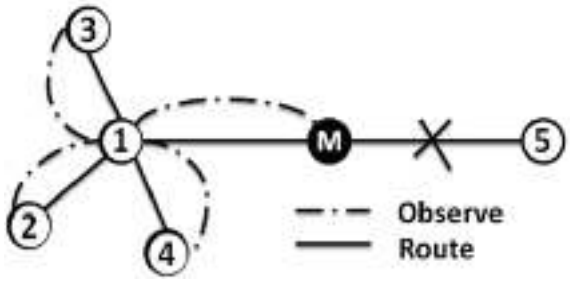


Fig 4: Neighbor node observation model

The watchdog mechanism is used to figure out the neighbor observation model for calculating DTV of each node

DTV Algorithm

Steps:
1. Node i watches node j from Tn to Tn+1
1. ($\Delta\alpha$,$\Delta\beta$,$\Delta\ \beta\ \gamma$) is calculated
2. Compare $\Delta\alpha$ and $\Delta\beta$ to decide the value of Θ using Eq.(4)
3. Compare the trust evidence (αn+1. Bn+1, γn+1) at Tn+1 using Eq.(1-3)
4. Calculate DTV of node j using eq. (5-8)
5. If Bij-Mij>η1 and Sij<ε1

Node j is trusted

Else if Bij-Mij<η2 and Sij<ε1

Node j is acting as malicious node and put it into MT .

Else

Node j is listed on ST table

End

α n+1 =(1-Θ) αn+$\Theta\Delta\alpha$ (1)

$\beta n+1 = (1-\Theta)\,\beta n + \Theta\Delta\beta$ (2)

$\gamma n+1 = (1-\Theta)\,\gamma n + \Theta\Delta\gamma$ (3)

$\Theta = \{\Theta 1$ if $\Delta\alpha >= \Delta\beta$ (4)

$\Theta 2$ if $\Delta\alpha < \Delta\beta$

$\Theta 3$ if $\Delta\alpha >= \Delta\beta$ then $\Delta\alpha < \Delta\beta$ }

$Bij = \alpha n / \alpha n + \beta n + \gamma n$ (5)

$Mij = \beta n / \alpha n + \beta n + \gamma n$ (6)

$Sij = \gamma n / \alpha n + \beta n + \gamma n$ (7)

$Dij = (Bij, Mij, Sij,)$ (8)

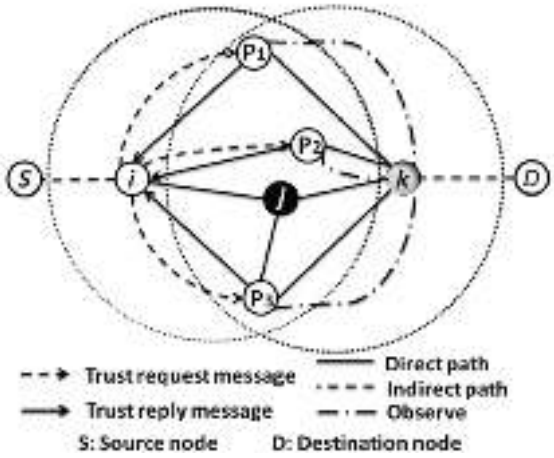


Fig.5: Neighbor Recommendation Trust Model (NRTM)

To figure out the co-operative black hole attack neighbor recommendation model is companied with IDV is used.

ITV Algorithm

Steps:

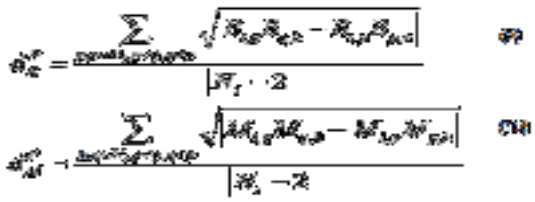
1. Do DTV alogithm on node j, if it acts normal go on to step 2
2. Node i ask node p's DTV on node j
3. Calculate the evaluation difference using eq (9)-(10)
4. Calcuate the ITV's of node j using eq (11)-(14)
5. Combine different ITV's using eq (15)-(18)
6. If $b_{i,k} - m_{i,k} > \delta 1$ and $s_{i,j} <$ □2
   Node k is trusted

Else if $b_{i,k} - m_{i,k} > \delta 2$ and $s_{i,j} <$ □2

Node k is malicious node and put into malicious table

Else

Node k is listed on suspicious table

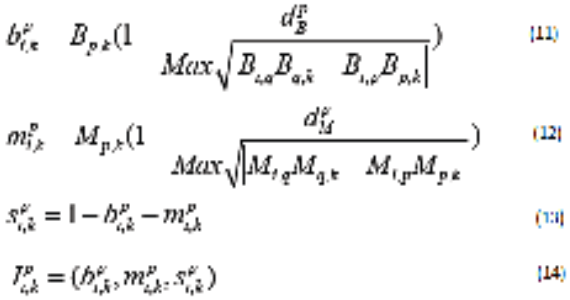


Where:

d_B^P: The evaluation difference of B in DTV

d_M^P: The evaluation difference of M in DTV

Ni: The neighbor nodes set of node i



Where:

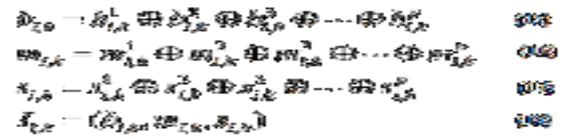
$b_{i,k}^P$: The benevolent actions ITV of node k through node p at present Tn

$M_{i,k}^P$: The malicious actions ITV of node k through node p at present Tn

$S_{i,k}^P$: The suspicious actions ITV of node k through node p at present Tn

$I_{i,k}^P$: The ITV of node k through node p at present Tn

According to the DS combination rule of more then two evidences the ITV's are combined together for finding combine ITV and the ITV is calculated using following eq(15)-(18)



Where:

bi,k : The benevolent actions ITV of node k at present Tn

mi,k : The malicious actions ITV of node k at present Tn

si,k : The suspicious actions ITV of node k at present Tn

Ii,k : The ITV of node k through node p at present Tn

DempsterShafer 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.Dempster-Shafer Theory (DST) is a mathematical theory of evidence.There are three important functions in the dempstershafer evidence theory:

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

-The belief function(Bel).

-The Plausibilityfunction(Pl)

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

  m:P(X) [0,1] →

- The belief function (Bel)

  Bel(A) = ∑B|B⊆Am(B)

- The plausibility function(Pl)

  Pl(A) ∑B|B∩ A =▪ m(B)

5. CONCLUSION

Today's 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]Dempster-Shafer Evidence Theory Based Trust Management Strategy against
Cooperative Black Hole Attacks andGray Hole Attacks in MANETs.

[2] Steven Abney. Dependency grammars and context-free grammars. manuscript.

[3] 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.

[4]Eliminating co-operative black hole and gray hole attacks using modified EDRI table in MANET, vaniA.hiremani,ManishaMadhukar Jadhav,2013

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