IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 3, March 2016.
www.ijiset.com
ISSN 2348 – 7968

# Defending Malicious Node Using Manets In Cooperative Bait Detection With Onion Routing Protocol

**S.Abirami[1], S.Barani[2], B.Dhivya[3], D.Meena[4]**
[1]Assistant Professor/CSE, [2,3,4] UG Students/ECE
Selvam College Of Technology, Namakkal

## ABSTRACT

Wireless networks are computer networks, which are connected by the cables. This is connected into buildings or different equipment locations. Mobile Ad-hoc Network (MANETs) is don't have any infrastructure which is used to communication purpose. Wireless network having many attacks. one specific attack is black hole attack and gray hole attack. Malicious node is fake node this do work when messages not send to the destination but it give fake acknowledgement this is also called as black hole attack. Gray hole attack is also called as at the same time sending packets are hake. To resolve this problems by using Dynamic Source Routing (DSR) is used to find out the new path simultaneously send data to the destination without hake which is referred to the Cooperative Bait Detection Scheme (CBDS). It having proactive and reactive scheme. CBDS implement reverse tracing techniques. These techniques used to find out the malicious node. Our proposed is implementing The Onion Routing (TOR). This makes encapsulated with encrypted data in multiple layers, and then send data with more security.

**Index Terms**: Black hole attack, Gray hole attack Dynamic Source Routing(DSR), Cooperative Bait Detection Scheme(CBDS),Malicious node, Mobile Ad-hoc Network(MANETs), The Onion Routing(TOR).

## I.INTRODUCTION

Mobile Ad-hoc Networks (MANETs) used in military operations and emergency. It don't have infrastructure and also used as communication. Malicious node is hake data from source and it gives fake acknowledgement to the destination. DSR used to create a new path then transmit data with security. Reverse tracing techniques used to detect malicious node. This checks all nodes get RREQ then detect which node don't get request .That node is called malicious node then it is removed by using reverse tracing technique method. Multiple malicious node make collaborative attack it damages the hole network which removes by CBDS. Collaborative Bait detection used to detect more number of attacks and it can used to remove the malicious node.

## II.PROPOSED APPROACH

Black hole attack is defect the hole network. Malicious nodes falsely present in the network and it hake data from the transmission. Reverse tracing then detect malicious node then it can be removed by this method. Dynamic Source Routing(DSR) detect a new path then send data that particular way and it refers to Cooperative Bait Detection Scheme(CBDS) that having proactive and reactive method. When process is doing it controls the transmission that is called as proactive. Process goes on a particular stage it will give response that is called as reactive. Bait is used to find the malicious node, this is the one type of case and detect one neighbor node.

Cooperative Bait Detection Scheme (CBDS) having steps are:

1. Initial bait step;

2. Reverse tracing step;

3. Shifted to reactive defense step;

4. The onion routing step.

The initial bait step and reverse tracing step is proactive defense step.

ISSN 2348 – 7968

## A.INITIAL BAIT STEP

Bait sending RREQ malicious node give RREP then find shortest path to send packets. To generate the destination address of the bait RREQ. The Source node selects the adjacent node .$n_r$ its one hop neighborhood node by taking address in destination address of the bait RREQ. Adjacent node is changed if the node moved; the bait would not remain unchanged. This is in fig 1.

If $n_r$ gave no reply RREP, it gives black hole list by the source node. The $n_r$ node sent reply RREP, it means malicious node not present in the network

.

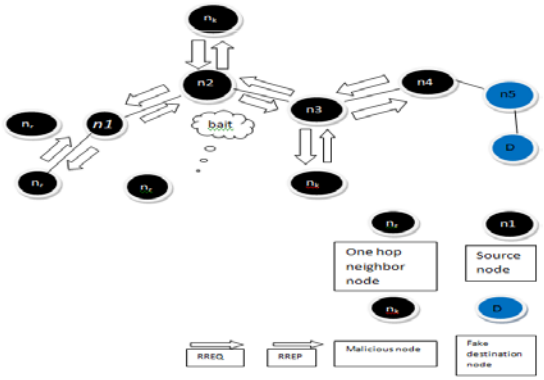



Fig: 1 Random selection of cooperative bait

## B.REVERSE TRACING STEP

The reverse tracing used to detect malicious node behavior to give reply to a RREQ. It will reply a false RREP. It used to detect the malicious node.

## C.REACTIVE DEFENCE STEP

After proactive defense step the DSR [10] route discovery process is activated. Destination is found that the packet delivery ratio is also reduced to the threshold, detection scheme would be detect for continuous maintanance and real time reaction efficiency.

Threshold value range is [85%, 95%] it is adjusted to the current network efficiency. Initial threshold value is set to 90%. Packet delivery ratio, routing over head, average end to end delay, through put is the performances matrices. This can be used to find the final outcome with more efficient. Packet delivery ratio is defined as the ratio of number of packet received by the destination and number of packets transmitted by the source. The amount of routing related control packets transmission to the amount of data packet transmission is also called as the routing overhead. The average time taken to the data transmission from the source node is called as the average end to end delay. The number of bits transmitted per second is called through put. The dynamic threshold algorithm to controls the time when falls the packet delivery ratio at the same threshold. The desending time is shortened, it denotes the malicious node presents in the network. At this time threshold value is increased. On the other hand threshold is reduced. CBDS observing the presence of malicious node it drop the packets or not drop. The dropped packets are neglected then malicious node create a gray hole attack that detect by CBDS and also detects all attacks.

**Algorithm for reactive defense phase float threshold value =0.9;**

```
Initial Defense ();

Float dynamic (threshold)

{       Float T1, T2;

        T1=calculate the time of PDR down to threshold;

        If (PDR<threshold)

        Initial defense ();

        T2=calculate the time of PDR down to threshold;

        If (T2<T1)

        {               If (threshold<0.95) threshold=threshold+0.01; else {

        If (threshold>0.85)

        Threshold=threshold - 0.01;  }
```

ISSN 2348 – 7968

If (simulation time<800 {return threshold; dynamic (threshold); } }

## III.THE ONION ROUTING

The onion routing is used to researching, designing, building and analyzing anonymous communications systems. That resist the traffic analysis and outsiders (e.g. internet routers) and insiders(onion routing servers themselves. Onion routing prevents the transport medium from known about who is communicating with whom and the network the place of communicating. Then the content of communication is hidden then the traffic leaves the onion routing network.

Client: The user of the Onion Routing network

Server: The target TCP applications such as web servers.

A circuit is built one hop by one hop Onion-like encryption. Then gives AES key with each router messages are divided into equal sized cells, the specific router knows only its predecessor and successor only the destination (OR3) can see the messages, anywhere it does not know where the message is from.

Onion routing process is carried in the encryption process. The transmitting data are encrypted and also encapsulated, it devide more number of layers it send only AES key , the neighborhood node don't know about the input messages.

Source node send data to destination .the input message reached and also read only by the destination node. The intermediate node cannot read this messages, because it have more security by creating by the onion routing method.Messages are encapsulated and the datas are sending multiple layers

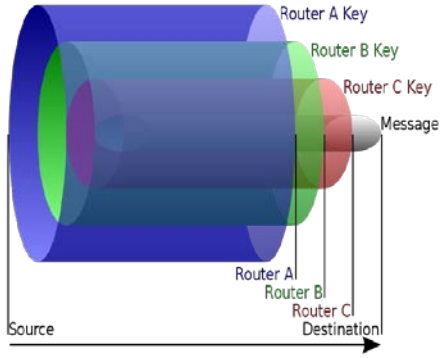
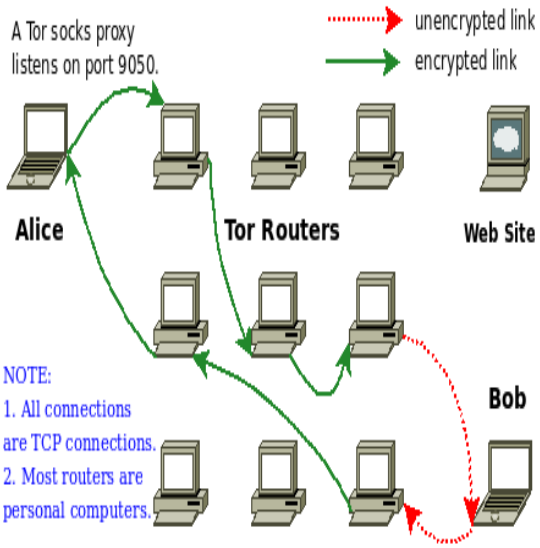
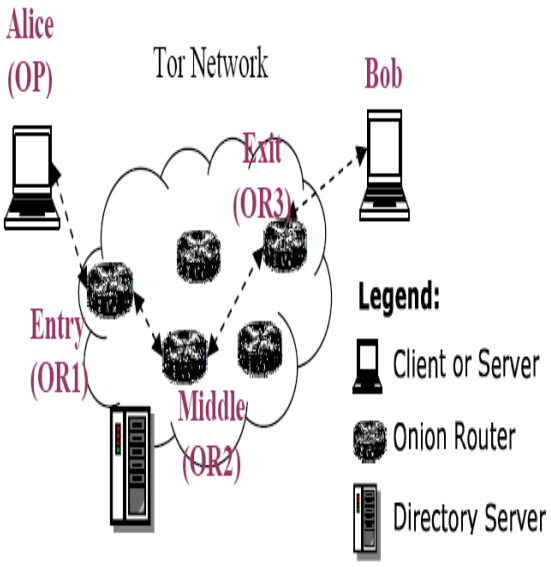



Fig: onion routing protocol



ISSN 2348 – 7968

## IV.CONCLUSION

This approach, we have proposed mechanism is (CBDS) for detecting malicious node by using MANETs the gray hole and black hole attacks can remove. The address of adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected by using a reverse tracing technique. This malicious node is put in black hole list. So that all other nodes that participated to the routing of the message passing are alerted to stop communicating with any node in the list. Using Tor(The onion routing) we can encapsulate the data when malicious node also cannot see the data. The previous works, the merit of CBDS lies in the fact that it works the proactive and reactive defensestep to achieve this goal.

## V.REFERENCES

[1]. P.-CTsou, J.-M Chang, H.-C. Chao, and J.-L. Chen, “CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture,” Wireless Communication, VITAE, Chennai, India, 2011.

[2]. S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol performance Issues and Evaluation considerations, March, 2013.

[3]. D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks,” Mobile Comput, 1996.

[4]. K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, “An acknowledgement based approach for the detection of routing misbehavior in MANETs,” IEEE Trans. Mobile comput., vol. 6, no. 5, May 2007.

[5]. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prrevention of cooperative black hole attacks in wireless ad hoc networks,’’in Proc. Int. Conf. Wireless Netw., Jun. 2003.

[6]. K. Vishnu and A. J Paul, “Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks,’’ Int. J. Compute. Appl., vol. 1, no. 22, 2010.

[7]. H. Weerasinghe and H. Fu, “Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation,’’ in Proc. IEEE ICC, 2007.