ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization Vol. 5, Special Issue 6, July 2016

4th National Conference on Design Innovations for 3Cs "Compute-Communicate-Control"

Organized by

Dept. of ECE, MVJ College of Engineering, Bangalore-560067, India

Detection of Malicious Nodes by using Reverse Trapping Technique in MANETs

R.Guruprasanna[1], M.Sujatha[2]

PG Student [DEC], Dept. of ECE, MVJ Engineering College, Bengaluru, Karnataka, India[1]

Associate Professor, Dept. of ECE, MVJ Engineering College, Bengaluru, Karnataka, India[2]

ABSTRACT: The term MANETs is a most popular. And MANETs networks is widely used in the many applications such as hospitals, military and education etc. Each independent node in the MANET can communicate with the other node without any wire connections. In the presence of malicious nodes in the MANET, Leads to serious security problem because it will disturb the entire routing processes. So in this paper we are introducing a new method to solve this problem. This paper gives a new method called CBDS [co-operative bait discovery method] to detect a malicious attack caused by malicious nodes in the MANET, and establish the efficient route in the network to carry the data from source node to destination node without any data loss. In this newly introduced CBDS method the reverse trapping method is implementing to detect the exact location of the malicious node in the MANETs. The newly introduced CBDS method simulation results are showed, this simulation results of our CBDS method is compare with the existing scheme called DSR scheme in relations of delay, routing overhead, PDR (Packet delivery ratio) and finally Throughput.

KEYWORDS:CBDS [co-operative bait discovery scheme], MANETs [mobile ad hoc networks], DSR [dynamic source route], RREP [Route Response], RREQ [Route Request].

I.INTRODUCTION

The mobile ad-hoc networks is most widely used technology in wireless applications such as entertainment, education etc. The unique features of the MANETs are it has the capability of self-organizing and independent organization. During, transmission of data between the nodes in MANET, the cooperation between nodes is also very important feature in MANETs. Because in Manet each node works as host and also acts as a router. This important feature also sometimes comes as dangerous problem during the data transmission, because if the malicious nodes is present in the network, this nodes occurs a disturbance to entire routing process. The below figure 1, shows the effect malicious nodes in the MANETs these malicious nodes which are present in the network attract the entire data packets by sending fake route response. By this false RREP the malicious nodes carry the selected data packets to other un-defined destination or false destination [1]. In generally these malicious nodes introduce two types of attacks in the network. They are blackhole attack and grayhole attack. In black hole attack, The malicious nodes which are present in the network can captured the entire data packets from source node and send this captured data to un-defined fake destination this creates a damages in the routing process. But in the grayhole attack initially malicious nodes are not detected but in later by the dropping of the date in PDR the grayhole attack will be detected. In this paper we are concentrated on grayhole and blackhole attack detection caused by malicious nodes. And establishment of an effective path between nodes by using the DSR [dynamic source route scheme] [1].

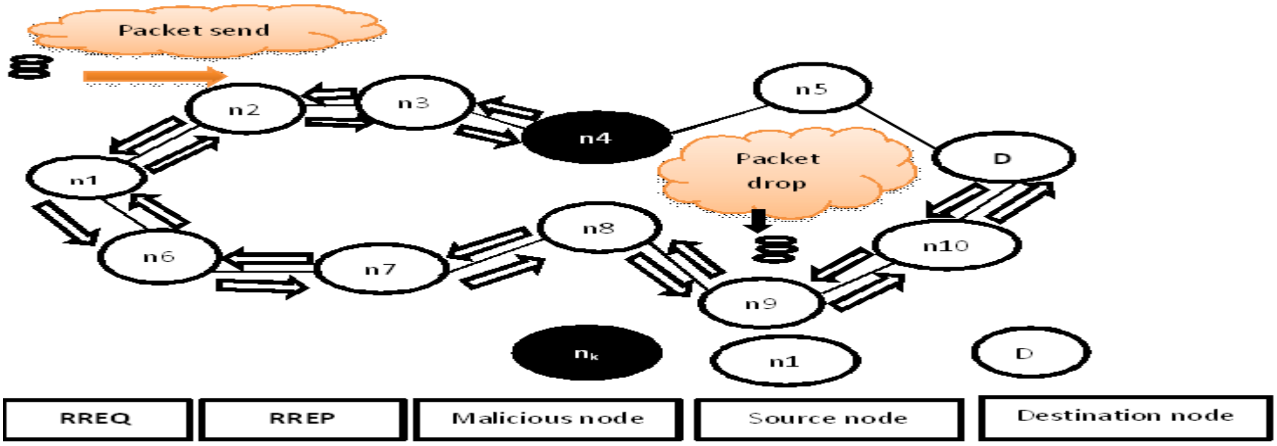

Figure 1: attracting data packets by sending false RREP

Initially the source node sends a path request or route request [RREQ] to all nodes. When this path request reaches the all nodes, each node in the network gives the route responses to that request. During that path response time each nodes in the MANET adds its entire address information in that RREQ packet. This RREQ packet consist of route record with in that route or path record, the address information of each node will be store. When the destination node receives this path request packet, then destination node will get know about in between nodes address in the whole route. After the destination node receives the route or path request packet [RREQ], immediately it sends a path response [RREP] to source node. This path response packet contains the entire routing information. And within this route or path response packet contains the entire information of established route between source node to destination node. If the RREP packet contains any false or fake destination address then source node will get know the fake destination address replied node is malicious node. Now we, are introducing a new method called CBDS [co-operative bait discovery scheme]for detection of malicious attack in the WSNsIn this new method we are used an address of the neighbour node as bait terminus address to attract the malicious node in the network to send a path response or route response [RREP] to source node. And in this new method we are using a new technique to trace the exact location of the malicious nodes in the network, that technique is called REVERSE TRAPPING TECHNIQUE for detecting malicious nodes in the MANETs. The detected malicious nodes by this technique are kept in the blackhole list, and send alarm to all nodes which are present in the network. After receiving of this alarm message by all nodes in the network. Each nodes stop the communication with the nodes which are present in the blackhole list.

.II.SYSTEM MODEL

The new introduced method, initially the source randomly selects all nodes which are present with in the network. And this source node use a neighbour node address as the bait address to detect the address of the malicious node to send path response or route response packet. . In this CBDS detection method the malicious node is detected and avoid the participation of malicious node can be achieved by the reverse trapping technique. This reverse trapping technique initiated when the dropping of packets occur in the packet delivery ratio. After the Malicious node is detected by reverse trapping, an alarm message is send all nodes. And put that malicious node in the blackhole list. All nodes will receives that alarm message and stop with the communication the nodes which are present in that blackhole list. And the important feature of this CBDS method is, it takes the advantage of both pro-active and re-active detection schemes. By this using of both the detection scheme in single mechanism the resources which are used for the detection mechanism is very less such as time and cost.This CBDS method is mainly based on the DSR technique. Due to the presence of malicious nodes in the network, the source will forward the entire data packets the un-authorised destination via fake path. This may leads occurring of blackhole attack in the network. To avoid this blackhole attack in the network the HAI message is added to packet information in CBDS. This adding of HAI message in the CBDS method to help respective node can recognize their neighbour nodes with single hop. And by adding this HAI message the source node get all information about each nodes present in the network, and by this address information of all nodes malicious nodes is detected. The detection of malicious node by CBDS mechanism can be achieved by 3 stages.1) Initial bait stage, 2) Reverse trapping stage, 3) Reactive defence stage.

A. Initial Bait Stage

In this initial bait stage illustrated in below figure 2.

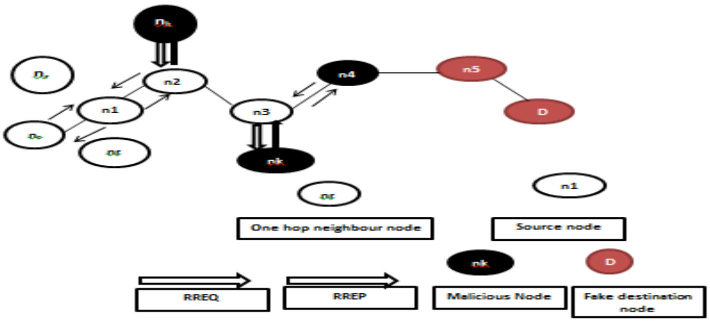

Figure: 2: Initial bait detecting by random selection of nodes by source node

This initial bait stage, initially done by the source node. First, the source node chooses the neighbour nodes randomly. The above figure 2 shows this random selection of nodes by the source node. In figure 2 source node selects a neighbour node $n_{r,}$ within its single hop neighbourhood nodes and source node exist the cooperation with this node by sending the RREQ [route or path request]. Each baiting is done randomly and neighbour nodes can change but bait is constant in the entire process. If the malicious attack is not caused by the node $n_{r,}$ after the sending of path request or route request then it shows that, the node n_r is not a malicious node. But if source node receives path response from any other node except the node n_r. This shows that still malicious nodes present in the network and now the reverse trapping is initiated to detect the position of malicious node. If suppose source node sends a path or route request to node n_r directly, if it is not reply for that path request then source node directly listed that node to blackhole list that indicates that node n_r is maliciousnode in that path.

B. Reverse trapping stage

This reverse trapping is new technique using in the CBDS detection method. By using this reverse trapping technique the detection of exact position of malicious node in network is done. This reverse trapping technique is initiated, during the source node send the route or path request into the network and get the path response from each nodes which are present in the network. The response packet RREP contains any false destination address immediately this reverse trapping technique starts its function and detects the position of malicious nodes in network. This CBDS method is more effective scheme to detect malicious nodes in the network compare to other existing methods. Because this CBDS method can capable to detect more than one malicious node in the network by using reverse trapping technique.Figure 3 shows, detecting of malicious node by using the reverse trapping technique. The node n4 is the malicious node in the network .This n4 malicious node send fake response to source node along with entire address list Q={node n1, node n2, node n3, node n4, node n5,node n6}.This node n4 can reply with $K4^{\prime}$= {n5,n6},this $K4^{\prime}$ Represents the entire information of the route to destination node. And now, the node 3 test and deleted the $k4^{\prime}$,After the receiving of path response. After the intersection $k4^{!}$ By source node. Now the unsure path information Z replied by malicious node is detected.

$$Z = K1^{\prime} \cap K2^{\prime} \cap K3^{\prime} \ldots\ldots\ldots\ldots \cap K_k^{\prime}$$

These malicious nodes which are present in the network give path response to every path or route request [RREQ]. Before detected a malicious node, the nodes which are present in the route is temporarily trusted. These provisionally trusted set Y is obtained by the difference of both sets Q and Z

$$Y=Q-Z$$

Initially, the source node confirms the presence of malicious node in the network by sending the test packet into the network. When path test packet enter to the network it rechecks the neighbour node that neighbour node sends the test packet to another node until this packet reaches the last node in Y. This happens to detect exact position of malicious node in the network. After the receiving of test packets up to last node, each node sends their route response to source node. If the route response contain any fake destination that node considered as a malicious node and listed in blackhole list. And send alarm message to other nodes to stop communication with that black listed node.

In figure 3, shows the network containing a only one malicious node that is $n_{k.}$ This node n4 sends fake route response to source node with the address list Q={Node n1, Node n2, Node n3, Node n4, Node n5, Node n6}. And then these malicious nodes select another fake node n5 by intentionally. This fake path detection by source node interact the received $K_k^{\,l}$ to obtain Z. And node n2 will send the request to n3 to know where the node is sending the packets. If the packets are sent node n5 to n3 through n4, then the source node stores this node to black list. In the figure 3, if the nodes n4 and n5 are cooperative malicious nodes. Then the T=Q-S = {n1,n2,n3} would be obtained, then n2 send the RREQ to n3 to listen to which node n3 sending the packets, either n5 or n6 identified. After the detection of fake node immediately cooperation with that fake node is stopped and send alarm mess to all nodes to stop communication with that fake node and establish the efficient route path from source node to destination node in the network

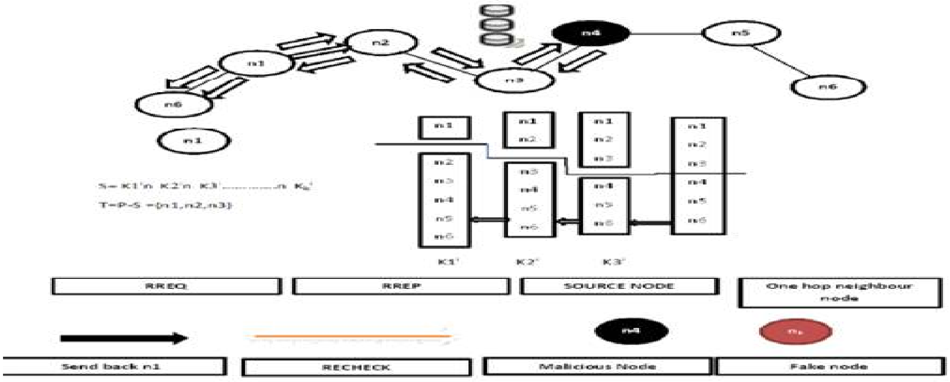

Figure: 3: Reverse tracing approach of CBDS scheme..

C. Reactive Defence Stage

After the completion of initial pro-active defence, The DSR starts its function, mainly the DSR function is route discovery, after this completion of above stages the DSR is initiated. While the way was established between the source to destination node. During data transmission of data from source node to destination node, if dropping occurs in packet delivery ratio immediately the detection method is initiated and detect the in which node data is dropping. This method defined the threshold 95%. The flow chart of entire mechanism is shown in figure 4

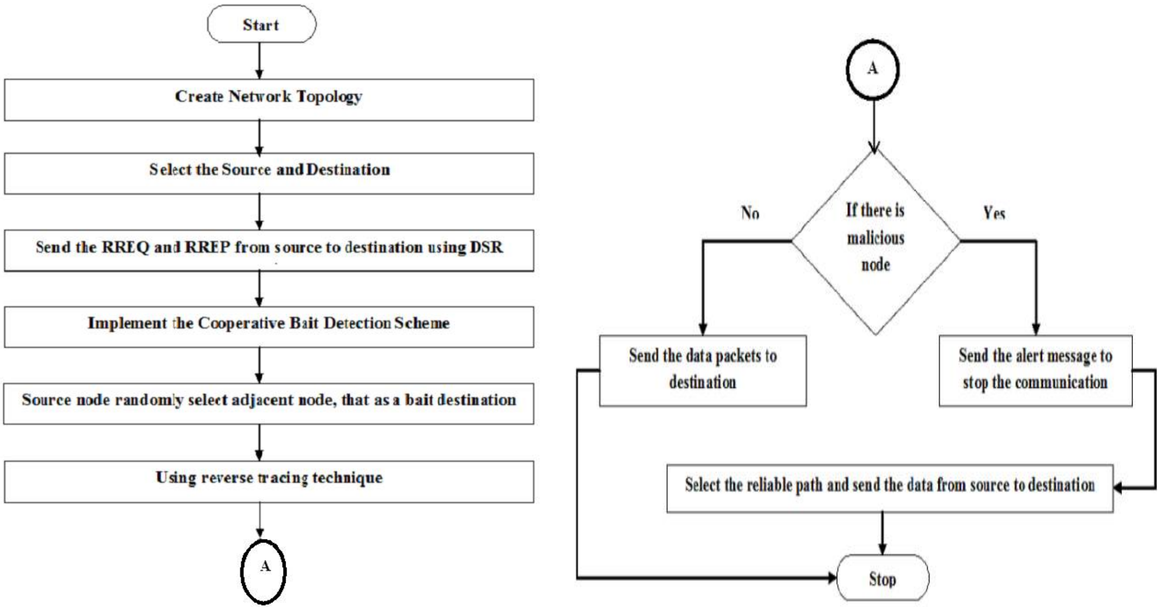
Start
Create Network Topology
Select the Source and Destination
Send the RREQ and RREP from source to destination using DSR
Implement the Cooperative Bait Detection Scheme
Source node randomly select adjacent node, that as a bait destination
Using reverse tracing technique
A
A
If there is malicious node
No
Yes
Send the data packets to destination
Send the alert message to stop the communication
Select the reliable path and send the data from source to destination
Stop

Figure: 4: Flow chart of CBDS mechanism

III.RESULT AND DISCUSSION

i. Simulation parameters.

To, study the simulation parameters of our newly introducing method called co-operative bait discovery method, we are using tool NS 2.33 [network simulator].these parameters of our CBDS method is shown in table I.

Table I: Simulation parameters

Constraints	values
Packet size	1000KB
Number of nodes	33
Malicious nodes	0 TO 40%
Pause time	0Sec
Area	1000m*1000m
Threshold	Dynamic threshold algorithm

i. Performance parameters of CBDS method.

In this Paper, we compared the performance parameters of newly introduced method of CBDS with existing scheme the DSR. In terms of parameters PDR[packet delivery ratio] and delay, routing overhead and finally the parameter throughput First, the below figure 5, shows the effect of malicious nodes in the network on the parameter PDR.

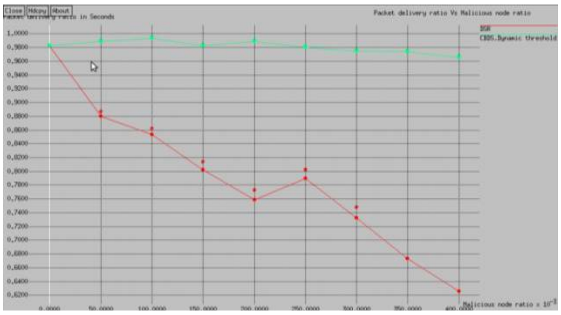

Figure 5: Comparison DSR and CBDS method on parameter PDR

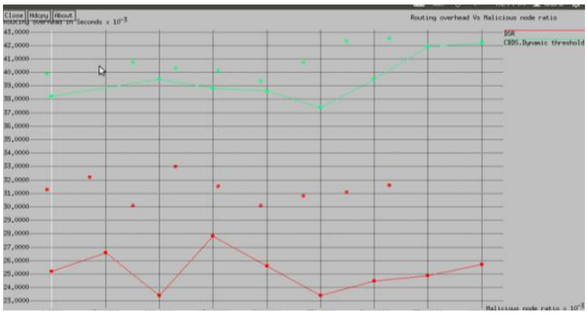

Figure 6: Comparison of routing overhead between CBDS and DSR

Compare to CBDS, The existing DSR scheme does not have any capabilities to protecting the data by malicious attack in the MANETs. If more number of malicious nodes present in the network our, CBDS method give high PDR ratio than existing systems. Next, Will disuses the other parameter of the CBDS method called RO [routing overhead. The figure 6, shows the results of this 2 schemes. Compare to CBDS, DSR produce a less routing overhead. Because in CBDS method it takes the use of both pro-active and reactive detection both during detection of malicious nodes in network. But in DSR, there is no higher capable detection schemes are used. Third, We study the important parameter called throughput. The figure 7 shows the throughput of the both the methods.

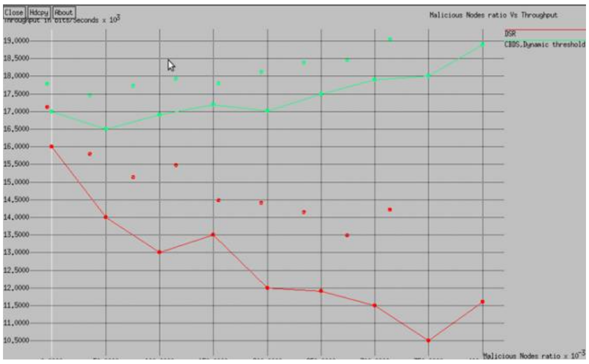

Figure 7: Comparison of throughput between and DSRCBDS and DSR

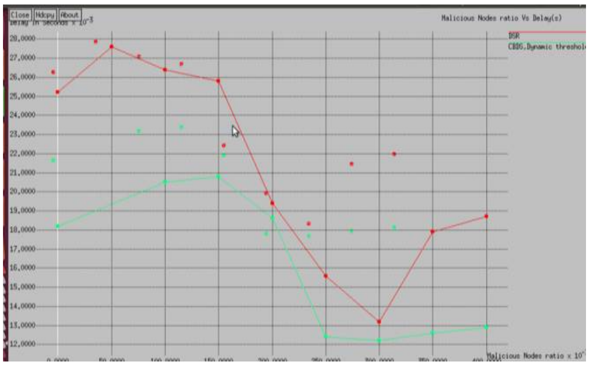

Figure 8: Comparison of end to end delay between CBDS DSR

The above figure shows the CBDS scheme achieve more throughput than the DSR, because if multiple malicious nodes present in the network DSR method fails to survive from that malicious attack. Finally, the last parameter is delay. The comparison of parameter delay between CBDS and DSR methods showed in Figure 8. In this delay parameter the CBDS scheme will produces less delay compare to DSR because this CBDS method capable to detect multiple malicious node in MANETs.

IV.CONCLUSION

In this, paper we proposed anew mechanism called Cooperative bait detection scheme [CBDS] for detecting the malicious node in MANET under gray/collaborative blackhole attack. And in this detection method takes the use of both proactive and reactive detection techniques. By using this CBDS mechanism, our simulation results are compare with the existing system called DSR method in terms of PDR [packet delivery ratio],RO[rotting overhead], Delay and lastly throughput.

REFERENCES

[1] P.C. Tsou, J.-M Chang, H.-C Chao and J.-L.Chen,"A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defines architecture,"in Proc.2nd Intl. Conf.wireless comm,VITAE, Chenai, India, Feb. 28-Mar., 03,2011,pp.1-5.

[2] I. Rubin, A. Behzad, R Zhang, H. luo, and E. Caballero,"TBONE: A mobile-backbone protocol for ad hoc wireless networks," in Proc. IEEE Aerosp. Conf.,2002,vol.6, pp.2727-2740.

[3] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks,"Intl. J.Comput. Sci. Inf. Security, vol. 7,no.1, 2010.

[4] W. Wang, B. Bhargava, and M Linderman, "defending against collaborative attack packet drop attacks on MANETs,"in Proc. 28th IEEE Int.Symp. Reliable Distrib, Syst., New Delhi, India, Sep. 2009.

[5] K.Liu,D. Pramod, K. Varshney, and K. Balakrishnan,"An Acknowlodgement based approach for detection of routing misbehaviour in MANETs,"IEEE Trans,Mobile comput., vol 6,no. 5,pp. 536-550,May 2007.

[6] D. Johnson and D.Maltz,"Dynamic source routing in ad hoc wireless networks,"IEEE Trans, Mobile Comput.,pp. 153-181,1996.