ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5 Issue 6, June 2016

Avoiding Blackhole Attacks Using CBDA Approach in MANETS

Aurhors- ***Ms.Shireen S, Mr.Kiranbabu T S, Assit.prof.***

Abstract: In mobile ad hoc networks the main requirement is building the connection between the available nodes such away they should communicate with each other .in such case if any malevolent node is present In communication network that may extend to security concerns. Malicious nodes may interrupt the routing operation .malevolent nodes may create the collaborative black hole or grayhole attack in the network in such instance preventing and detecting nodes launching attacks is a very difficult .defending Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach resolve this problem by designing a dynamic source routing based mechanism it is a Cooperative Bait Detection Approach here it collude together the advantages of reactive and proactive defense architecture. CBDA algorithm uses the initial bait step and reverse tracing method to detect the malicious node launching the collaborative blackhole/grayhole attack in the network in this scheme in presence of malicious node attack the CBDS will exceeds the results of DSR t .2ACK.Best fault tolerant routing protocol methods in terms of routing overhead or packet delivery ratio.

Keywords: mobile adhoc network(MANETS).CBDS approach.DSR Routing.

1. Introduction

Nowadays mobile devices are widely available these devices have been using for various important application. Such application includes emergency preparations and response operations etc... because of infrastructure less property of mobile adhoc networks (MANETS).in order to organize

The wireless local area network nodes present in entire network should cooperate with each other while performing transmission operation. While receiving and transmitting the data these features may lead to serious security concern, if any malicious nodes present in the entire network those nodes will cause malfunctioning of entire network.

Most of research work concentrated on the security of MANETs these research work deal with detecting and preventing the collaborative attacks .such approaches will become weak when multiple malicious nodes collude together creates damages to network. Mobile adhoc network are highly vulnerable to routing attacks such as blackhole/grayhole because of infrastructure less property and dynamic topology feature of MANETS .malicious nodes itself broadcast information that it has shortest path to the destination .it will pull all packets by using false message of shortest path after receiving all packets it will discard the packets without forwarding to destination and intercept the entire routing process.

2. Related Work

Many research works shown the trouble in detecting the malicious nodes those cause collaborative attack in the network most of

research works investigate solution fan the single malicious node or else these require lot of resources to detect the nods creating collaborative block hole/gray hole attack in terms of time and cost all the available methods so for used for detecting the malicious nodes are divided into two broad categories

1) proactive detection scheme these is need of monitoring the all the nodes constantly to detect the attack in such case increases the overhead of detection and research used in the entire operation constantly wasted but proactive detection scheme will help to detect the attacks in the initial stage 2) Reactive detection scheme when these is significant drop accurse in the pocket delivery ratio then reactive method will get trigger among these both reactive and proactive schemes one investigated that is considered as benchmark schemes for the purpose of comparison Liu ct al investigated a method of 2Aek for detection of misbehavior of nodes in the MANETS 4) In order to indicate that the data pockets received successfully this method will use tow-hop acknowledgement packets are sent opposite direction of routing operation but this scheme produces the extra overhead.

This is a kind of proactive method the acknowledgement ratio Rack is use to control the received data packet.xue and Nahrstedt investigated best effort fault tolerant method .in this scheme source will chose the new path if any problem occur in the existing path but still there may be chances of existence of malicious node in the new path and this method also has the drawback of routing overhead

3. Proposed approach

In CDBA mechanism it will aim to detecting malicious node launching Black Hole / Gray Hole attack in the routing path IN this approach source node statistically selects the adjacent node.

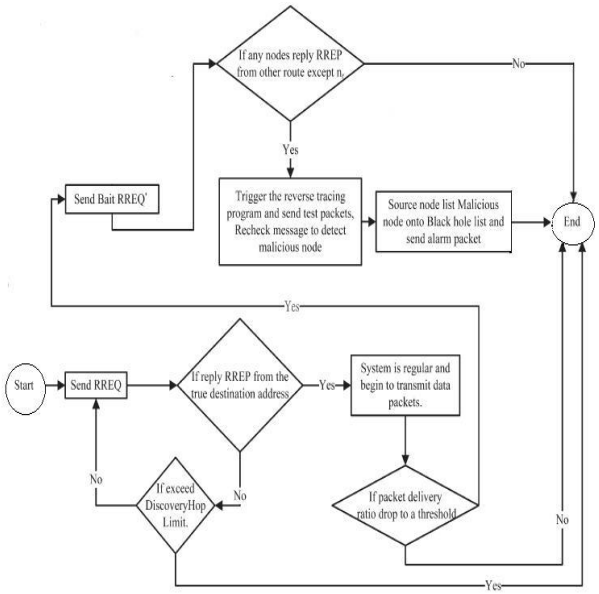

Figure 1. Architecture diagram of CBDA

The CBDA approach uses the initial bait and reverse tracing techniques, in initial bait step it will use the bait address to get to know malicious node present in the network or not, once if it got the doubt about the presence of malicious node in the network it will perform the reverse tracing technique to find out exact which node is malicious in the network .the CBDA algorithm merges both advantages of proactive and reactive in initial as well as in subsequent step respectively

Based on DSR approach the CDOA will work first it will record the address of all the nodes in the entire network by sending RREQ once it receive the RREP it will identify the address of all the nodes in the network which are sending pocket to destination after receiving message the source node may select the shortest path chosen by malicious node may result the black hole attack gray hole attack To find

out this attack CBDA user the initial wait step and reverse recovery and the shifted to reactive step

1. Initial bait step

Initial bait source node will send RREP request to get reply from the malicious node source node select neighbor node with one hop distance and co-operates with this node by taking in address as the destination

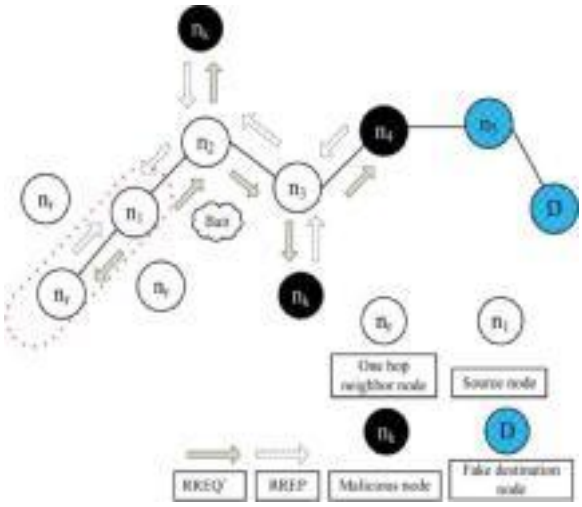

Fig. 2. Random selection of a cooperative bait address.

This has been shown in fig 2 if the adjacent neighbor node had not launched attack once the source node sent the packet RREQ' there will be reply RREP from some other node in along with the reply RREP from nr node extra information along with adjacent node RREP this information indicates that malevolent node present in a network if only reply comes from nr node it will record that there is no malicious node in the network if source node receives reply from some other node after sending bait request RREQ' it will show the malicious node in the network in such cases the reverse tracing method in next step is used to find out the malicious node in the routing path

2. Initial reverse tracing step

To detect the malicious node reverse tracing program is used. malicious node will send the false RREP after receiving RREQ' this program will apply for those nodes which RREP to catch the temporary trusted path and dubicious path information and CBDS is able to detect more than one malicious node in the network for ex.if n_m is malicious node in the network it may give false reply RREP an address list $P = \{n_1, . nk, . . . n_m, . . . n_r\}$ is recorded in RREP. If nk node gets the RREP it will separate the destination address nk with the address list P. The destination address will store in IP field and collect the address list Kk={ n_1, n_2, n_3, nk } recorded in reply packet and difference also recorded in the reply packet ie.

$$K'_k = P - K_k = \{nk_{+1} . . . n_m, \ . . . n_r\}$$

Where K'_k will show the information to the destination node then the information will send to the source node .the same information will store in the "Reserved field" of K'_k to conform the received data is from which node nk will check the source address in the IP fields of the RREP the next hop of nk in address list P and one hop of nk.If source address in RREP not same in next hop address list P and next hop nk then it will perform forward back method , n_4 node will reply $K_4' = \{n_5, n_6\}$, this reply will send to the next node n3,once the source node intersection set K'_k' the path information provided by the malicious node will be detected by performing intersection operation i.e.,

$$S = K_1 \cap K_2 \cap K_{3,,,} . . \cap K'_k.$$

Before that malicious node send RREP to all the nodes present in route before all nodes assumed to be trusted to gain temporary set T. i.e., T=P-S Now source node need to confirm which would send the test packets and recheck messages towards the last node

in temporary trusted list T. Once the source node had recorded a promiscuous mode to listen to which node is the last node in T sent the packets to and has sent the same reply back to source node. Then source node will add the node in blackhole list and broadcast the alarm packet through the network by this it will inform all the nodes to stop there routing process .

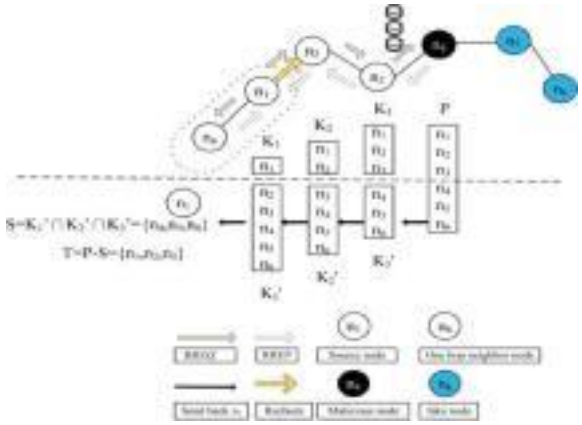

Fig. 3. Reverse tracing program of the CBDS approach

The fig 3 shows all the situations when single malicious node n_4 arrives in the routing path Once the source node n_1 sends RREQ the malicious node n_4 will send false reply with the address list

$$P = \{n_1, n_2, n_3, n_5, n_4, n_6\}$$

Node n4 randomly will select node n_5 which is filled by n_4.again if node n_3 had got the RREP message it will separate the destination address n_1 with address list P and get the address list $K_3 = \{n_1, n_2, n_3\}$ again the node will perform the difference operation to acquire $K_3 = P - K_3 = \{n_4, n_5, n_6\}$, after this node n_3 would reply to source node n_1 with K_3' and RREP similarly node and n_1 will perform the difference operation and obtain K_2 '= { n_3, n_5, n_4, n_6} and K_1'={ n_2, n_3, n_5, n_4, n_6} respectively. All the differences will send to source node, this will perform intersection to gain the dubious path information of the malicious node S= $K_1 \cap K_2 \cap K_3 = \{n_4, n_5, n_6\}$ is obtain then source node again will do difference operation i.e., T=P-S to get temporary set at the end.

Source node will send test packet to this path and recheck message to next node n_2 inform this node to listen and enter the premiscous path to find out that n_3 has diverted packets to node n_4 and node n_2 will send the listening information to the node n1 then source will put the source node in blackhole list .if malicious node selects some other node in its RREP these nodes will be added to the blackhole list. Similarly here, n_5 node will be added to the blackhole list because it is randomly selected by the malicious node n_4 by performing same intersection S= $K_1 \cap K_2 \cap K_3 = \{n_4, n_5, n_6\}$ and difference operation. By CBDS approach more than one malicious node in the network

C. Shifted Reactive Defense Phase

The DSR route discovery process is activated once the proactive process get completes .if there is drop in packet delivery ratio .i.e., to the threshold according to the network efficiency the value of threshold will be adjusted.

The dynamic threshold algorithm will be designed when packet delivery ratio falls within the initial threshold value.

4.Simulation Results.

Scenario 1:

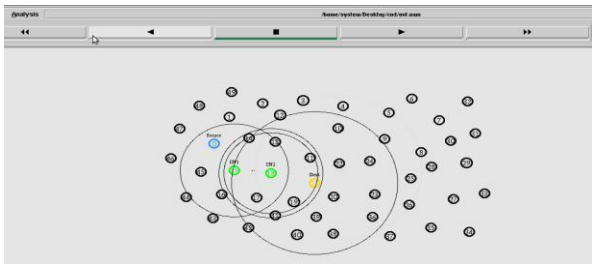

Fig4.initial stage source node and destination node

Initially we created topology and selected source node and destination node.

Scenario 2:

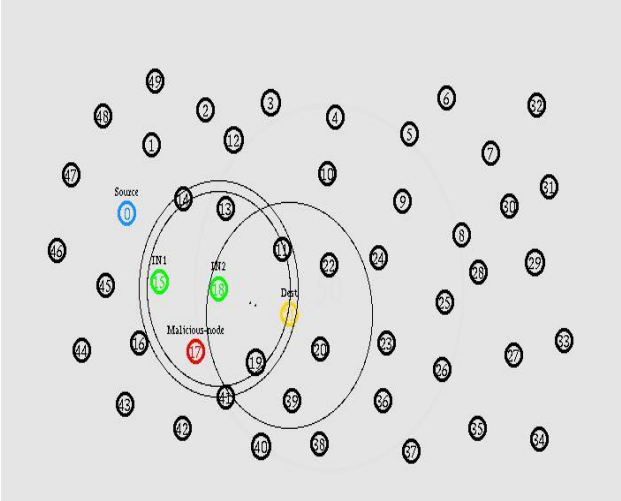

Fig.5. when malicious node exist in the topology

Above fig shows one more extra node its malicious node. Whenever malicious node exists in the network simply it will add packets to routing process. And sends reply RREP back to the source node.

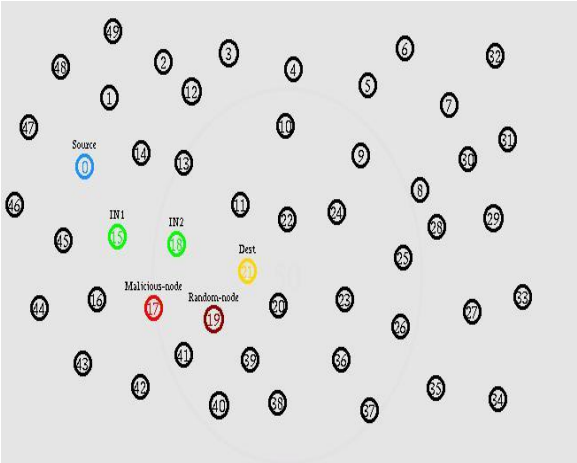

Fig.5. malicious node select random node to send packets

Again the malicious node may select some other node randomly it will divert packets to random node.

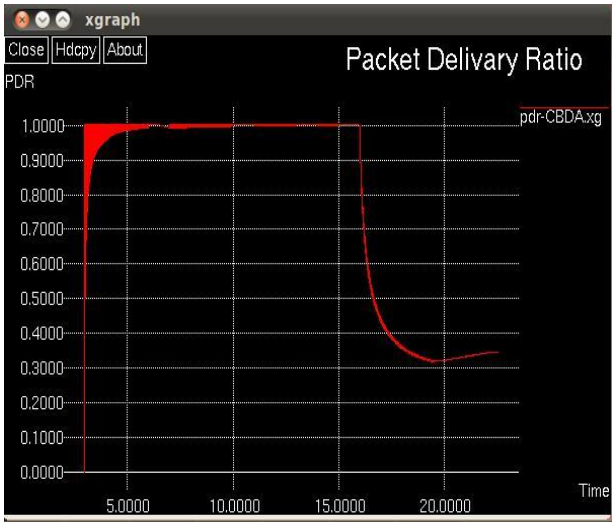

Fig.7 shows packet delivery ratio of CBDA scheme

Above graph shows the packet delivery of CBDA which shows packet delivery ratio. i till malicious node exist in the network packet delivery ratio is high once the malicious node exist it will start degrading.

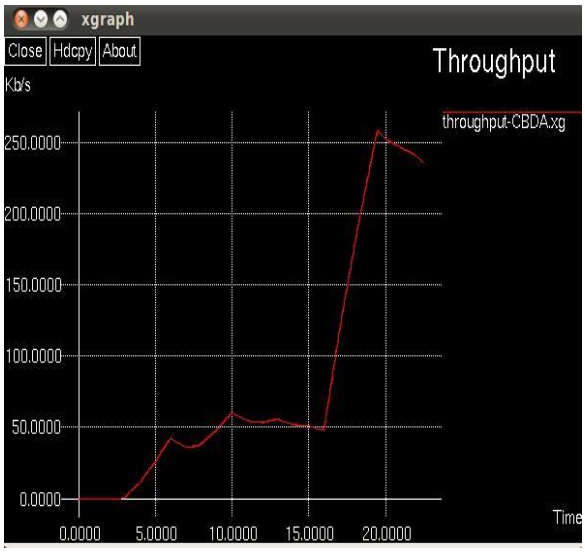

Fig 7.shows throughput of the CBDA scheme

Above graph shows throughput of the entire operation .which shows high throughput by using CBDA operation.

5.Conclusion

our proposed scheme discovers better results in terms of packet delivery ratio and throughput which exceeds the results of DSR,2ACK,BFTR approaches. Our future intention is to apply this approach to some other collaborative attack and intended to integrate the some other security approaches to provide security to MANETS adhoc networks.

5.Referances

[1] P.-C. Tisou, J.-M. Chang, H.-C. Chao, and J.-Li. Cihen, "CBDS: A cooperative bait detection scheme to prevent malicious node forMANET based on hybrid defense architecture," in *Proc. 2nd Intl. Conf. Wireless Commun.*, *VITAE*, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1– 5.

[2] S. Corison and J. Mackier, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013). [Online]. Available: http://www.elook.org/coimputing/rfc/rfc2501.html

[3] C. Chaing, Y.Wang, and H. Chaoi, "An efficientMesh-based core multicast routing protocol onMANETs," *J. Internet Technol.*, vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[4] D. Johnision and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.

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

[6] A. Baadiache and A. Belimehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile iad hoc networks," in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265.

[8] K. Vishnu and A. J Pauil, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," *Int. J. Comput. Appl.*, vol. 1, no. 22, pp. 28–32, 2010.

[9] K. Liu, Di. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based apprioach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[10] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002.

[11] S. Raimaswamy, H. Fu, M. Sreekantaradhya, J. DixoBn, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575.

[12] H. i and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networkowss: Simulation implementation and evaluation," in *Proc. IEEE ICC*, 2007, pp. 362–367.

[13] Y. Xue and K. Nahirstedt, "Providing fault-i ad hoc routing service in adversarial environments," *Wireless Peris.Commun.*, vol. 29, pp. 367– 388, 200