ISSN (Online) : 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)
Volume 3, Issue 4, April 2017

Defending against various attacks in MANETs

[1]Shubhangi Patil, [2]Prof. Trupti Agarkar
[1] [2]Electronics Department, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai
[1]shubhvp23@gmail.com, [2]truptiagarkar07@gmail.com

Abstract :- **In MANETs various types of attacks are present. Which mainly affected on security. In this paper, we concentrated on how to avoid such attacks. Here mainly black hole and gray hole attacks are get eliminated. In network, malicious nodes are present which disturbs the communication. Such malicious nodes are first detected and then isolated, using CBDS method.**

Keywords: **- MANET security, attacks , overcome techniques.**

I. INTRODUCTION

MANET Stands for" Mobile Ad Hoc Network." A MANET is nothing but a type of ad hoc network that is capable to change locations and configure itself on the fly. Because MANETS are mobile Ad-hoc, so that they use wireless connections to connect the various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission [5].

MANET have been used for many vital applications because of the widespread availability of mobile devices. These applications are military operations and emergency as well as response operations. This is mostly happened because MANET has infrastructure less property. In a MANET, each node performs vital role, according to demand it acts as host as well as router. In such communication process for receiving data, there should be cooperation between nodes for forwarding data packets which forms a wireless local area network. These best features also have disadvantage which effects on security of network. Indeed, such applications brings some critical problems on the safety of network topology, data routing, and data traffic. The presence and cooperation of malicious nodes may break the routing process, resulting into bad functioning of the network operations. For security point of view of MANETs many researches works on this problem. Most of the researches focussed on prevention and detection of such malicious nodes. In this, the effectiveness of these researches not use full so that when multiple malicious nodes come together they begins a collaborative attack, which may result into more damages to the network. In wireless the absence of any infrastructure added with the MANETs dynamic topology feature makes the network insecure to the attacks of routing which are black hole and gray hole attacks. Gray hole attacks are nothing but variations of black hole attacks. [8]

Mobile Ad Hoc Network is the type of network used for mobile communication. For moving users whenever session not performing good and link get disturbed then MANETs used because it provides best performance. These are wireless networks for linking different networks. In this some of are linked to LANs and some to internet applications of the network. MANETs connect them without any wireless router.

Best features of MANETs [6] are as follows:

- Dynamic Topologies.
- Energy-constrained Operation.
- Limited Bandwidth.
- Security threats.

II. LITERATURE SURVEY

J. Sen: for gray hole attack detection, he used local cooperative anomaly detection [3].

Jian-Ming Chang et al: To avoid malicious node for MANET he used a Cooperative Bait Detection Scheme. Cooperative bait detection scheme (CBDS) is a mechanism used to detect malicious nodes which are launching black hole or gray hole attack [2].

K. Narang et al. have provided mechanism for detection of black hole attack. Data Routing Information (DRI) table used to detect cooperative black holes which get verified by intermediate nodes and source nodes [8].

G. Wahane et al.: Cooperative black hole attack detection mechanism is provided by him. Cooperative black holes is detected by Data Routing Information (DRI) table and get verified by True Link. The True Link method is totally dependent on timing constraint. DRI table is maintained by every node in the network [4].

ISSN (Online) : 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)
Volume 3, Issue 4, April 2017

Jian-Ming Chang et al.: have provided a technique which effectively detects the malicious nodes that try to launch gray hole/collaborative black hole attacks. The address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, done using CBDS technique [1].

A. Bhattacharyya et al.: Various types of attacks in Mobile ADHOC Network has explained by him. And, explained Prevention techniques for such attacks. These attacks have entered from both internal side of the network and from the external side of the network [7].

III. ATTACKS ON MANET

DATA traffic attacks and CONTROL traffic attacks are the two main types of attacks. This classification of attack is normally based on the goal of attack and their characteristics.

A. DATA traffic attack

Black hole attack:

Here, attacker node behaves such as a Black hole node, it drops each packet coming to it and energy vanishes from our universe into a black hole. In this the attacker node is acts as an intermediate node between two parts of communication and then breaks the communication [7].

Gray Hole Attack:

There are two phases in gray hole attack. In the first one, AODV protocol is used by malicious node to introduce itself as having shortest correct route to the destination node. It is having same purpose of intercepting packets even with bad route. In the second one, malicious nodes drop the coming packets with some probability. But this attack is very hard to find than black hole attack. A gray hole attack may show its malicious behaviour in various ways.

B. CONTROL traffic attack

The other types of attack, such as traffic attacks or jamming attacks, this is not CONTROL attack. They are a part of physical layer security protocols.

IV. METHODS TO OVERCOME ATTACKS IN MANET

Cooperative Bait Detection Scheme (CBDS)

The cooperative bait detection scheme (CBDS), which used for detecting and preventing malicious nodes which creates gray hole/collaborative black hole attacks in MANETs. Here adjacent node is selected by source node with which it must be cooperate. Such address is used as bait destination address to bait malicious nodes to send a reply RREP message. By using a reverse tracing technique such Malicious nodes are thereby detected and prevented from taking part into the routing operation. In this, an alarm is sent by the destination node to the source node for triggering the detection mechanism as a significant drop occurs in the packet delivery ratio. CBDS method is DSR-based method. After receiving RREP message from the destination node source node can recognize all node addresses. But the source node may unable to find the intermediate nodes that has the routing information to the destination or the reply RREP message or the malicious node reply forged RREP. This results in that source node may sending packets through that shortest path which is selected by the malicious node, which may then create a black hole attack. To resolve this problem, the HELLO message concept is added to the CBDS for helping each node which are adjacent within one hop. This utilize the reverse tracing program of the CBDS to identify the exact addresses of malicious nodes. Such baiting RREQ packets are same as to the original RREQ packets, except that their destination address is the bait address [1] CBDS method has three steps: (1) initial proactive defence- the initial bait process; (2) initial proactive defence initial reverse tracing process; and (3) shifted to reactive defence phase- the DSR route discovery Starting process. The procedures of each step are explained below [1][2].

Initial proactive defense- the initial bait phase:

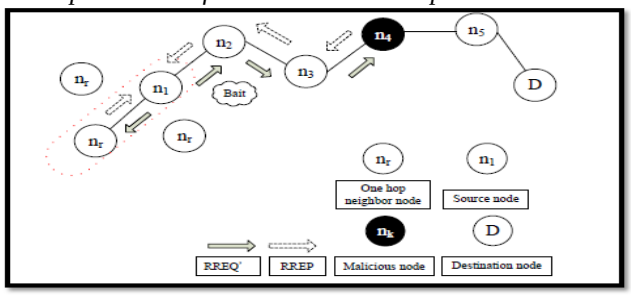

Figure 1: Randomly choose a cooperative bait address and send bait RREQ [1]

When node sends the bait RREQ it enters bait phase in order initialize routing. Here firstly malicious node, nr node, which not create black hole attack would be detected. When source node sent RREQ the other nodes in the network also gives reply besides nr node. Which gives the presence of malicious nodes in routing, as shown in Fig.1. So that by using reverse tracing phase is started to find out this route. In such process if and only if nr node gives reply means there were no other malicious nodes present in the network.

ISSN (Online) : 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)
Volume 3, Issue 4, April 2017

And in this if only nr node gives reply it meant that there were no other malicious nodes and then the DSR routing started the program of finding shortest path. Whenever the other nodes as well as nr node send RREP then there was reverse tracing process is started for detecting route. If nr node does not gave reply to RREP, source node [1][2] immediately listed it onto black hole list.

Initial proactive defense- initial reverse tracing phase:

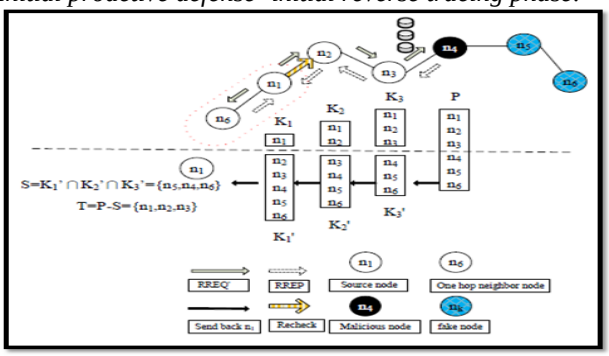

Figure 2: The reverse tracing program of CBDS [1]

In this phase, malicious nodes are found which are going from the path. Because they are replying to RREQ. After receiving the RREQ node keep that address in the path storage field, and this address list Q = n1,..nk observed in the area is stored into the route cache. The malicious gives response to source node request with false RREP. So that reverse tracing operation is kept for reducing the suspicious path information and temporary trusted area in the route. Here it is assumed that all the nodes in the route are trusted nodes before giving reply to RREP. In this subtraction process of P and S we get the set of trusted nodes, T=P-S. In this source node recheck message to the second to last node in T and sent test packets to this route. Here the node must have entered a trusted mode to find which is the last node in T and then sent the packets to it and the result again to the RREQ node. Then the RREQ node would listed such node to the black list and such information is broadcasted into the network in the form of alarm packets. This happens to aware all nodes about malicious nodes, and dropped such RREP packets. Instead of diverting if the last node dropped the packet then source node listed such node into the black list.

The source node n1 wish to send packets to the destination node n6, here a single malicious node n4 existed. As soon as n1 sending the RREQ malicious node n4 sent a false RREP message with the address list P= (n1, n2, n3, n4, n5, n6). n5 was a random node filled in by n4. If n3 received the replied RREP by n4, it would conduct the set difference operation with K3= (n1, n2, n3) for calculating P-K3= K3'= (n4, n5, n6). This then send reply message to K3 and the source node n1 based on the routing data in P. Likewise, n2 and n1 also do the same process after RREP to obtain K2' = (n3, n4, n5, n6) and K1'= (n2, n3, n4, n5, n6). This then again send to source node for communication purpose. Here the suspicious path data of the malicious node, S = (n4, n5, n6) was obtained. The source node then performed this calculation P-S=T= (n1, n2, n3) to obtain a temporarily trusted set of nodes. At the end, for rechecking purpose the source node sent the test packets to this path and requesting n2 to enter the promiscuous mode and listening to n3. After that it came to the result that n3 diverts packets to malicious node n4. Such listening results n2 reverts to the n1. Then source node n1 list the n4 to black hole list.

n5 and n4 are two available cooperative malicious nodes. Like above examples, T=P-S= (n1, n2, n3) can be obtained, and node n2 listen to which node n3 send the packets. In this, either n5 or n4 would be detected, so that their cooperation procedure get stopped. The other nodes can be baited by other source nodes in MANET [1][2]and detected.

Shifted to reactive defense phase:

As soon as the initial proactive defence phase over route discovery procedure get followed by using DSR technique. So that route is established. After that, if at the destination node packet ratio is falling the threshold value then the detection mechanism is performed again. Here threshold value is changing, which can be managed according to network efficiency. Such that malicious nodes of the both gray hole and black hole attacks [1][2] can be detected by using CBDS method.

Complete CBDS procedure as follows:

Overall working of this CBDS method is shown by using flow chart.

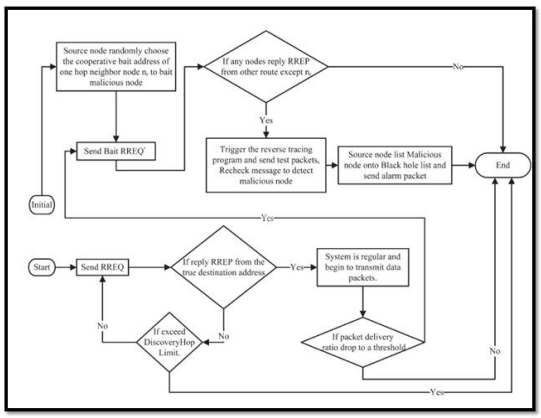

Figure 3: Operations of the CBDS [1]

ISSN (Online) : 2395-2717

International Journal of Engineering Research in Electrical and Electronic Engineering (IJEREEE)
Volume 3, Issue 4, April 2017

V. PERFORMANCE ANALYSIS

Here performance of network checked by using the throughput parameter. Throughput is the ratio of total amount of data received by destination from source to the total time required to receive it.

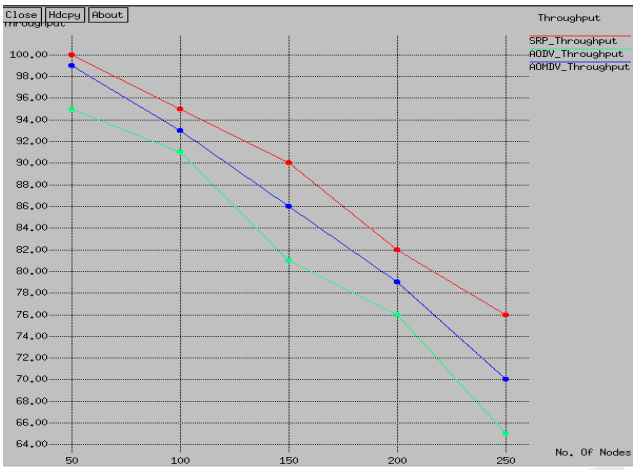

Figure 4: Throughput Graph

VI. CONCLUSION

In this paper, detection mechanism of malicious nodes is discussed. Also, various attacks are discussed. Here CBDS method is used which is combination of both proactive and reactive defence architectures. By using bait address concept, it baits malicious nodes and such nodes are detected by using reverse tracing techniques and helps to avoid black hole and gray hole attacks.

VII. FUTURE WORK

Except gray hole and black hole attacks other data traffic attacks will also be reduced by using this system. By reducing probability of false detection some of the data traffic attacks will also be reduced.

REFERENCES

[1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach, IEEE SYSTEMS JOURNAL, VOL. 9, NO. 1,MARCH 2015..."

[2] P.-C. Tsou, 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, in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28Mar., 03, 2011, pp. 15.

[3] Jaydip Sen, M.Girish Chandra, Harihara S.G., Harish Reddy, P.Balamuralidhar, A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks, MIPRO 2014, 26-30 May 2014, Opatija, Croatia.

[4] Gayatri Wahane, Ashok M. Kanthe, Dina Simunic, Technique for Detection of cooperative black Hole Attack using True-link in Mobile Ad-hoc Networks, IEEE-ICCIC 2014 ISBN: 978-953-233-081-6 Year 2014.

[5] http://techterms.com/definition/manet

[6] http://techupdates.in/what-is-manet-characteristics-and-applications-of-manet-incommunication

[7] Aniruddha Bhattacharyya, Arnab Banerjee, Dipayan Bose, Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques Department of Computer Science and Engineering, Institute Of Engineering and Management, Saltlake.

[8] Er.Kiran Narang, Sonal, A study of different attacks in MANET and discussion about solutions of black hole attack on AODV protocol, International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) Volume 2, Issue 4, April 2013.

[9] W. Al-Mandhari, K. Gyoda, N. Nakajima, Wired and Wireless Communication, Adhoc On Demand Distance Vector (AODV) Performance Enhancement with Active Route Time-Out parameter WSEAS TRANSACTIONS on COMMUNICATIONS Manuscript received Feb 12, 2008; revised Aug 10, 2008

[10] L. Tamilselvan and Dr. V Sankar Narayana, Prevention of black hole attack in MANET, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communication, IEEE, 2007.

[11] S. Sen, J. A. Clark, and J.E. Tapiador, Security Threats in Mobile Ad Hoc Networks. Department of Computer Science, University of York,YO10 5DD,UK.

[12] N. P. John , A. Thomas, Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review,

International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012.