ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Preventing Manet From Blackhole And Grayhole Attacks Using Reverse Tracing Technique

Pathan Aiyaz Khan
M.Tech Student
Department of IT
Sreenidhi Institute of Science and Technology(Autonomous)
Hyderabad, India.

Mr.M.Dhanaraju
Assistant Professor
Department of IT
Sreenidhi Institute of Science and Technology(Autonomous)
Hyderabad, India.

Abstract

Network which is not connected by any type of cable is a wireless network. The main purpose of using wireless network is that it enables users to avoid the cost of introducing cable lines in the building or making connection between different locations. These networks are highly affected by network attack.

One of these attacks are black hole attacks in which malicious node claims that it has the fresh and shortest path. As MANET doesn't have any standard infrastructure and the dynamic topology that makes these networks highly susceptible to security flaws like exploiting vulnerabilities to routing protocols and transferring harmful packets in the networks. These security issues results in adverse effect on this network. Now the task is to prevent MANET from these security threats. As this paper is based on DSR protocol hence we developed a scheme called the Cooperative Bait Detection Scheme (CBDS), which directly focus on detection and prevention of malicious nodes introducing gray hole/black hole attacks in MANETs.

To implement this CBDS we use back tracing method. Hence from our proposed system we won't require any special hardware or detection node to prevent againt blackhole attacks.

Keywords- ***Cooperative bait detection scheme (CBDS), collaborative blackhole attacks, collaborative bait detection, detection mechanism, dynamic source routing (DSR), malicious node, grayhole attacks, mobile ad hoc network (MANET).***

1. Introduction

Nature of MANET is a collection of mobile, self organized and non-centralized nodes. The infrastructure less and dynamic structure makes MANET easy to security related issues. A mobile ad hoc network (MANET), also known as mobile mesh network (MMN), which configure itself by wireless links. Because of its infrastructure-less nature, network management and routing is done collaboratively by the nodes i.e. total functioning of network is carried out by nodes [8] [9]. Topology of the network varies with respect to the mobility of nodes. Rather than, the security of MANET it have many flaws. This results the security of MANET being less than a cable network and causes many security issues. As MANET follows open communication medium which makes attacker easy to overhear transmitted message. Old routing protocol trustworthy to all nodes that will transmit data packet, in dynamic topology, with any decentralized infrastructure, and lack of authority which makes MANET susceptible to various types of attacks [11]. Black hole attack is most commonly used attacks in which malicious node attract all packets by using forged RREP which falsely claims that it has fresh and shortest route to the destination and later it discards the packet without forwarding it to the destination.

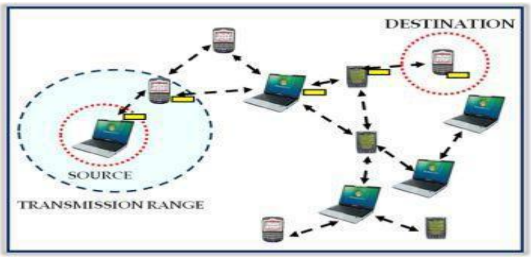


Fig 1: MANET Data Transmission

This paper resolves security issues by proposing CBDS method containing Proactive and reactive defense architectures, which randomly establishing a collaboration with neighbor node. The address of the neighboring node is used as the bait destination address, and the baiting malicious nodes is used by adjacent node for reverse tracing program to RREP and identify malicious node[11]. Ultimately malicious node is detected in the black hole list and block communication to further nodes. Hence, proposed scheme reduces packets loss that are caused by malicious nodes and comes with better throughput [1] [2]

2. LITERATURE SURVEY

Chin-Feng Lai et al, IEEE [2014]. This paper paper tries to resolve gray hole and black hole attacks caused by malicious nodes by implementing a Dynamic Source Routing (DSR) mechanism called as Cooperative Bait Detection Scheme (CBDS) which has pros of both reactive and proactive detection schemes to find malicious nodes as proactive detection scheme observes adjacent nodes and guards against initial stage attacks and reactive detection scheme activates only when there is drop in delivery ratio. Our goal is achieved by Reverse tracing technique by using cooperative bait detection scheme to detect malicious nodes in MANET for the black hole and gray hole attack. In this MANET mechanism every node has only its own state information and combine effect of the other nodes. In proposed mechanism we will be implementing multiple attackers with multiple defenders. This network perform computing operations without disclosing its input information to other devices, this computation is Secure Multiparty Computation (SMC) [4]. The drawbacks can be overcome by modification of data inputs to prevent eavesdropping. Another approach is to make the identity ambiguous to prevent it from other devices. The primary function of SMC solutions is to prevent the privacy of computation process. In this network attacks can be active or passive. MANET security network can be classified into 5 layers based on OSI model[5] as infrastructure layer, application layer and security layer, network security layer describing functions of every layer in intimately. Using OSI hierarchy we design security architecture of MANET. MANET's secure and reliable design is a result of inter coordination of layers of OSI for MANET.

3. PROPOSED SYSTEM

In this paper we are proposing CBDS detection scheme to find malicious node which causes black hole/gray hole and cooperative attacks. source node randomly selects neighbor node to mark that node as bait node and defense mechanism aggregates proactive and reactive defense structure. Bait destination address is used by the source node to find the malicious node in which malicious node sends RREP reply through reverse tracking scheme. Drop in packet delivery ratio enables detection mechanism and automatic alarm is set and triggered itself and capability of maintenance and immediately reactive response is achieved[2][11]. It enjoys pros of proactive detection in early stage and reactive response reduces waste of resources. In initial stage our mechanism doesn't uses reactive architecture which suffers black hole attacks. Although with DSR help we can find out all addresses of nodes in the route after RREP is received at source node. Nonetheless, the source node doesn't know exactly which intermediate node have routing route to destination node and reply RREP. This type of scenario makes the source node send packets to the shortest path that is claimed by the malicious node and later network suffer black hole attack which causes packet loss. Which malicious node causes loss in the network is not by the DSR. As compared to DSR method, the Hello message is used by AODV to identify which nodes are their neighboring nodes within one-hop[11][3]. To find the exact addresses of malicious nodes we send bait address to entice the malicious nodes and to provoke reverse tracing program of CBDS. In addition the baiting RREQ packets are created by source node. This paper tries to solve collaborative black-hole attacks by DSR-based routing mechanism, with the help of CBDS (Cooperative Bait Detection Scheme) that contains the advantages of both reactive and proactive defense architectures [11]. The source node uses any adjacent node address as the bait destination address is the approach of this paper[11] to find malicious nodes to entice send a RREP reply message back. By using reverse tracing technique we detected and prevented malicious nodes.

The CBDS scheme comprises three steps:
A. Initial bait step;
B. Reverse tracing step;
C. Shifted to reactive defense step

The first two steps are initial proactive defense steps, and the third step is reactive defense step.

A. In Initial Bait Step we seduce a malicious node to send a reply RREP back by sending the bait RREQ' where the malicious node advertise itself as having the shortest path to the destination node. Now the source node randomly selects the neighboring node i.e.nr in its one-hop neighborhood nodes and cooperates with the node by taking its address as the destination address for bait RREQ'. As the baiting is done randomly and there may be chances that adjacent node can be changed if that node moved, whereas bait would remain unchanged. This situation is illustrated in Fig. 2. If neighboring node nr knowingly doesn't give reply RREP, it would be directly enlisted in the black hole list by the source node. And if only the route reply RREP is sent by nr node, that means there is no any other malicious node in the network, and the route that nr has provided; in this case, DSR will start its route discovery phase. Route provided by the node nr to the route discovery phase will not be listed.

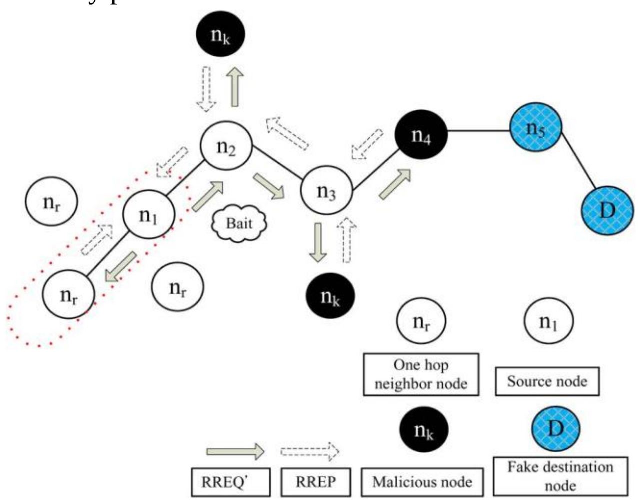


Fig 2: Random Selection of cooperative bait.

B. Reverse Tracing Step The behavior of malicious node is detected by the route reply to the RREQ' message in reverse tracing technique. A false RREP reply is sent back by the malicious node to the RREQ' message. To deduce the dubious path information to have temprorily trusted zone in the route reverse tracing operation is conducted for the nodes that receive RREP.

C. Reactive Defense Step from the above initial proactive defense steps (steps A and B), the DSR route discovery process is activated. Once the route is established and at the destination the packet delivery ratio significantly drops to the threshold, than the detection mechanism is triggered. The initial threshold value is set at 90%. But the threshold value is a varying in the range [85%, 95%] which can be set according to the current network efficiency. When there is packet delivery ratio fall under the same threshold we have designed a dynamic threshold algorithm. Malicious nodes are still present in the network if the descending time is not shortened. The threshold will be lowered in this case, to overcome this threshold should always be adjusted as upward.

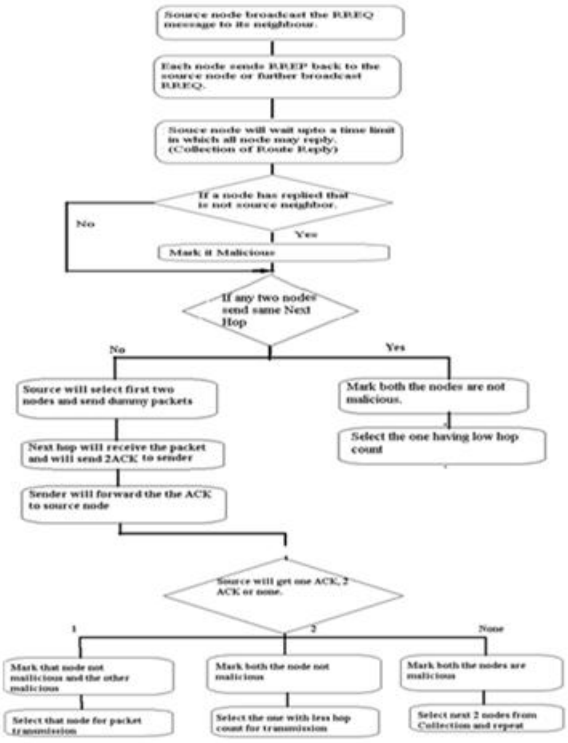

Source node broadcast the RREQ message to its neighbour.
Each node sends RREP back to the source node or further broadcast RREQ.
Souce node will wait upto a time limit in which all node may reply. (Collection of Route Reply)
If a node has replied that is not source neighbor.
No
Yes
Mark it Malicious
If any two nodes send same Next Hop
No
Yes
Source will select first two nodes and send dummy packets
Mark both the nodes are not malicious.
Next hop will receive the packet and will send 2ACK to sender
Select the one having low hop count
Sender will forward the the ACK to source node
Source will get one ACK, 2 ACK or none.
1
2
None
Mark that node not mallicious and the other malicious
Mark both the node not malicious
Mark both the nodes are malicious
Select that node for packet transmission
Select the one with less hop count for transmission
Select next 2 nodes from Collection and repeat

Fig 3: Reverse Tracking Flow Chart

Algorithm for Reactive defense method

```
float threshold=0.9;
initialDefence();
float dynamic(threshold)
{ float T1,T2;
T1=calculate the time of PDR all the way down to threshold;
if(PDR < threshold)
initialDefence();
T2=calculate the time of PDR all the way down to threshold;
if(T2 < T1)
{ if(threshold < 0.95)
threshold=threshold+0.01;
else {
if(threshold > 0.85)
threshold=threshold-0.01;
}
if(simulationTime < 800) {
return threshold;
dynamic(threshold);
}
else return 0.9;
}
```

Operations of the CBDS are shown in the below Fig. 4. From our CBDS mechanism it is observed that we find the dubious path of the malicious nodes as well as that of trusted nodes; Therefore nodes which sends RREP is marked as the malicious node and a trusted can be identified, whereas CBDS is capable of finding whether a malicious node will drop the packets or not. As a result malicious nodes launching gray hole attacks can be detected by the CBDS method and in the same way black hole attacks are detected.

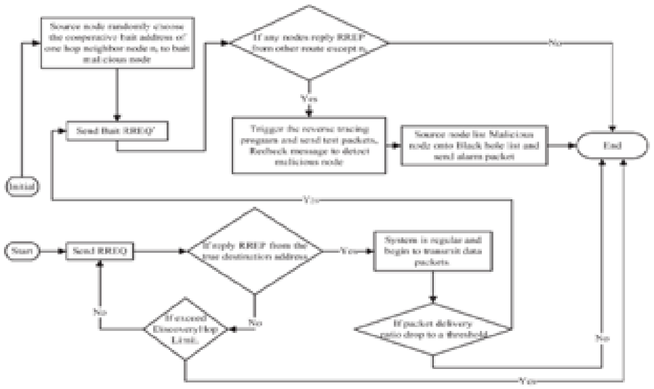
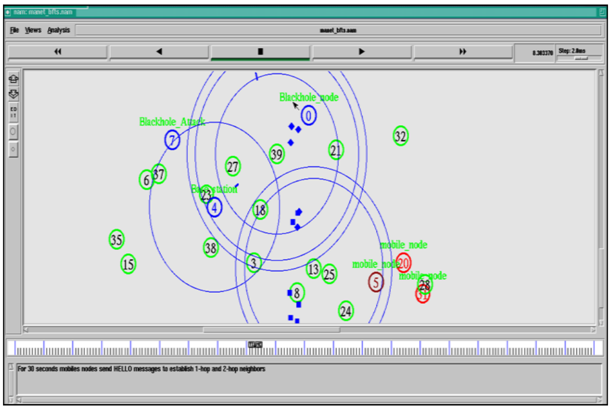

Source node randomly choose the cooperative bait address of one hop neighbor node n, to bait malicious node
If any nodes reply RREP from other route except n
No
Yes
Send Bait RREQ'
Trigger the reverse tracing program and send test packets. Recheck message to detect malicious node
Source node list Malicious node onto Black hole list and send alarm packet
End
Initial
Yes
Start
Send RREQ
If reply RREP from the true destination address
Yes
System is regular and begin to transmit data packets
No
If exceed DiscoveryHop Limit
No
If packet delivery ratio drop to a threshold
No
Yes

Fig 4: CBDS operations

4. PERFORMANCE EVOLUTION

Ns-2 simulation tool is used to understand the performance of our CBDS approach. Here we use the IEEE 802.11 MAC with channel data rate of 11 Mb/s. The default CBDS threshold in our simulation is set to 90%. Network used for simulations is shown in Fig. 5, in this we randomly select a node to perform attack in network.



For 30 seconds mobiles nodes send HELLO messages to establish 1-hop and 2-hop neighbors

Fig 5: NAM Results

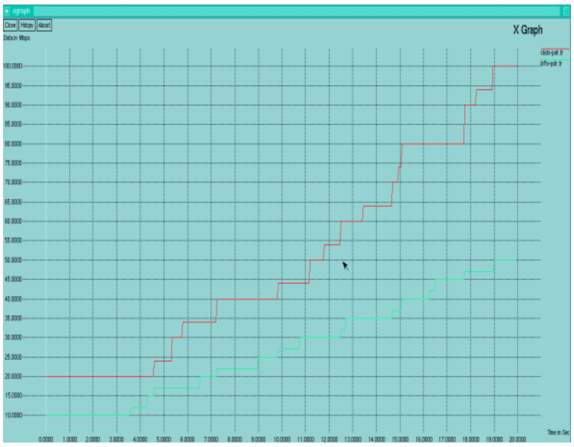


Fig 6: Packet Delivery Ratio

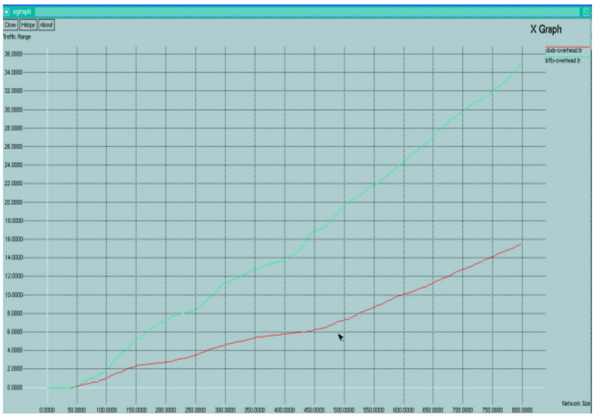


Fig 7: Routing Overhead

CBDS scheme here shows a higher packet delivery ratio compared with DSR. Instead there being 40% of hostile nodes, the CBDS mechanism can still successfully detect these hostile nodesin the network whereas keeping the packet delivery ratio at 90%. When the threshold is 95% that would result in earlier route detection rather than the threshold is 85% or the value is set to the dynamic threshold. Now we study the routing overheads of DSR and CBDS for different threshold Fig. 7. As we see Fig. 7, we can observe that as the number of malicious nodes increases, the DSR produces the lowest routing overhead as compared to the CBDS. As the matter of fact that DSR has no defensive mechanism or standard security method. Routing overhead produced by CBDS for different thresholds is bit higher that produced by DSR; this is because CBDS will first send bait packets, in its bait phase and then turn that reactive defensive phase afterward. A tradeoff should be made between packet delivery ratio and routing overhead. Thus we studied the reaction of thresholds on the routing overhead. When the threshold value is set to 95% it is found that routing overhead of CBDS reaches higher value. Compared to 95% threshold value CBDS triggers fast to that of the value set as 85% threshold value or it is equal to dynamic threshold. Bait packets can be sent many a times in the network. Dynamic threshold value can be set according to the network performance.

5.CONCLUSION

Here in the paper, we have learned the security threats that ad-hoc network faces and presented the security objective which must be achieved. On one side, the security-sensitive applications of an ad-hoc networks require high security on the other side, ad-hoc networks are highly vulnerable to security attacks. Therefore, as per the requirement of the network we need to make network more secure and robust The flexibility, ease and speed with that these networks can be set up to imply they'll gain wider application. This leaves Ad-hoc networks wide open for analysis to reach these demanding application. The analysis on MANET security continuous to be in its early stage. The prevailing proposals are generally attack-oriented in this they first identify all security threats and hence enhance the prevailing protocol or propose a new protocol to thwart such threats. As a result the solutions are designed expressly with the CBDS technique combines reactive and proactive detection schemes both which enhances its potency of detection. It may be deployed for both self deployed node topologies additionally as randomly deployed node topologies. It's a network wide detection scheme wherein on detection of malicious node the complete network is intimated regarding the detection by Alarm signal. CBDS has been successfully enforced on gray hole and black hole attacks before and has proved to be equally economical just in case of DoS attacks and Sleep deprivation attacks in our experiment too. Simulation result have shown an increased response and increased detection for CBDS.

The networking opportunities for MANETs are intriguing and also the engineering trade-offs are too many and difficult. This paper conferred a description of in process work and a vision for the long term and future integration of mobile networking technologies into the Internet. There's a necessity for standardized, secure, and practical routing and interface solution(s) for mobile networking support. The future holds the chances for deploying inexpensive, IP internetworking compatible solutions to create self-organizing, wireless routing materials for commercial and military use. In future work, CBDS may be deployed on various different security threats in MANET and it results may will be checked for validation. A small variation in throughput and end to end delay is determined just in case of CBDS that remains an area of additional improvement.

6.REFRENCES:

[1] Chin-Feng Lai, Han-Chieh Chao, Jian-Ming Chang, Isaac Woungang, and Po-Chun Tsou, Member, IEEE.Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach.

[2] BabakHosseinKhala, HamidrezaBagheri, Marcos Katz, Mohammad JavadSalehi, Mohammad Noor

mohammadpour, and Seyed Mohammad AsghariPari. A SelfOrganizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks. Rakesh kumar Sahu,Narendra S chaudhari "performance evaluation of ad hoc network underblack hole attack 978-1- 4673-4805-8/$31.00,IEEE 2012

[3]Richard Yu, Helen Tang, Minyi Huang and Yanwei Wang, Member, IEEE. A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks.

[4]Durgesh Kumar Mishra (Acropolis Institute of Technology and Research, Indore, India). Mahakal Singh Chandel (Arjun Institute of Advaced Studies and Research Centre, Indore, India), Rashid Sheikh. Security Issues in MANET: A Review.

[5] Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng College of Computer Science Chongqing University Chongqing, China. Research on MANET Security Architecture design.

[6] G.V.S.Raju and RehanAkbani, "Authentication in Wireless Networks", Proceedings of IEEE 40th Hawaii International Conference on System Sciences, 2007.

[7] Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile ADHOC Networks", International Journal of Computer Applications, Vol. 1, No. 22, 2010.

[8] Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", Journal of Computing, Vol. 3, ISSN 2151-9617, January 2011.

[9] Po-Chun TSOU, Jian-Ming CHANG, Yi-Hsuan LIN, Han-Chieh CHAO and Jiann-Liang CHEN, "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", ICACT, Feb. 2011.

[10] Radhika Saini and ManjuKhari, "Defining Malicious Behaviour of a Node and its Defensive Methods in Ad Hoc Networks", International Journal of Computer Applications, Vol. 20, April 2011.

[11] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen, "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture", IEEE, 2011.

[12] Ankita Gupta and Sanjay PrakashRanga, "VARIOUS ROUTING ATTACKS IN MOBILE AD-HOC NETWORKS", International

[13] Ramandeep Kaur, Jaswinder Singh,"Towards Security against Malicious Node Attack in Mobile Adhoc Network", International Journal of Advance Research in Computer Science and Software Engineering, volume 3, issue 7, july 2013.

[14] Navdeep Kaur ,Mouli Joshi "Implementing MANET Security using CBDS for combat sleep Deprivation & DOS Attack" International Journal for science and Engineering.