Defending Against Attacks in MANETs using Cooperative Bait Detection Approach

M. Ahmer Usmani[1], Manjusha Deshmukh[2]

Lecturer, Department of Computer Engineering, Bharat College of Enginerring, Badlapur, Mumbai University, India[1]

Proffesor, Department of Computer Engineering, Pillai Institute of Information Technology, Panvel, Mumbai University, India[2]

Abstract: Wireless networks are computer networks that are not connected by cables of any kind. The use of wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. Wireless networks are susceptible to many attacks. One such specific attack is a blackhole attack in which malicious node falsely claiming itself as having the fresh and shortest path to the destination. This paper attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal. Proposed system helps us in defending against the blackhole attack without any requirement of hardware and special detection node.

Keywords: Cooperative bait detection scheme (CBDS), dynamic source routing (DSR), Twice Acknowlegement (2 Ack), grayhole attacks, malicious node, mobile ad hoc network (MANET).

I. INTRODUCTION

Due to the widespread availability of mobile devices, mobile ad hoc networks (MANETs) [1], [3] have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure less property.

In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network [3]. These great features also come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations.

Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

II. PROPOSED APPROACH

Black hole is an attack in wireless network in which malicious node falsely claiming itself as having the fresh and shortest path to the destination attract traffic towards itself and then drops it. The proposed approach attempts to resolve this issue by designing a dynamic source routing [2](DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal.

The CBDS scheme comprises three steps:

1. the initial bait step;
2. the reverse tracing step; and
3. the shifted to reactive defense step,

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

A. Initial Bait Step

The goal of the bait phase is to entice a malicious node to send a reply RREP by sending the bait RREQ' that it has used to advertise itself as having the shortest path to the node that detains the packets that were converted. To achieve this goal, the following method is designed to generate the destination address of the bait RREQ'. The source node stochastically selects an adjacent node, i.e., n_r, within its one-hop neighborhood nodes and cooperates with this node by taking its address as the destination address of the bait RREQ'. Since each baiting is done stochastically and the adjacent node would be changed if the node moved, the bait would not remain unchanged. This is illustrated in Fig. 4.1.

If n_r deliberately gave no reply RREP, it would be directly listed on the blackhole list by the source node. If only the n_r node had sent a reply RREP, it would mean that there was no other malicious node in the network, except the route that n_r had provided; in this case, the route discovery phase of DSR will be started. The route that nr provides will not be listed in the choices provided to the route discovery phase.

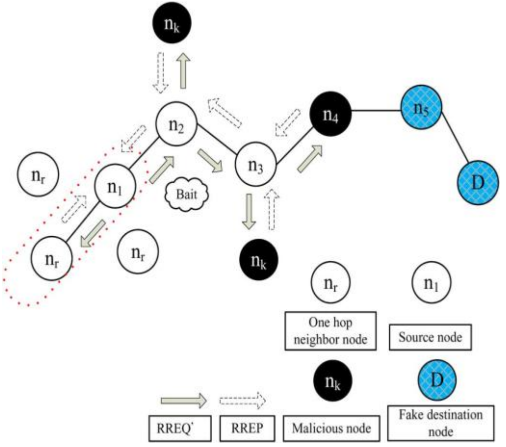

Figure 4.1: Random Selection of cooperative bait.

B. Reverse Tracing Step

The reverse tracing step is used to detect the behaviors of malicious nodes through the route reply to the RREQ' message. If a malicious node has received the RREQ', it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route.

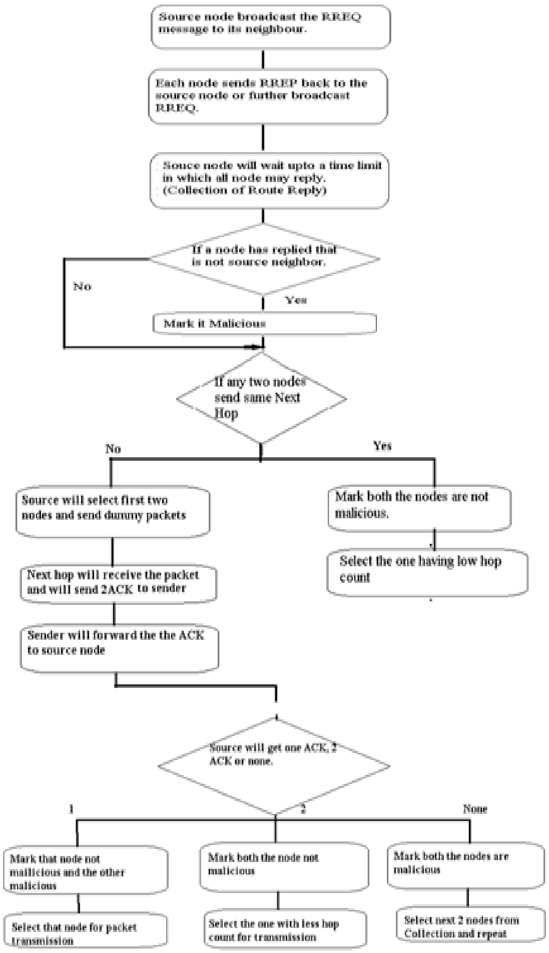
Source node broadcast the RREQ message to its neighbour.
Each node sends RREP back to the source node or further broadcast RREQ.
Souce node will wait upto a time limit in which all node may reply. (Collection of Route Reply)
If a node has replied that is not source neighbor.
No
Yes
Mark it Malicious
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

Figure 4.2: Reverse Tracing Phase

C. Reactive Defence Step

After the above initial proactive defense (steps A and B), the DSR [10] route discovery process is activated. When the route is established and if at the destination it is found that the packet delivery ratio significantly falls to the threshold, the detection scheme would be triggered again to detect for continuous maintenance and real-time reaction efficiency.

The threshold is a varying value in the range [85%, 95%] that can be adjusted according to the current network efficiency.

The initial threshold value is set to 90%.

We have designed a dynamic threshold algorithm that controls the time when the packet delivery ratio falls under the same threshold. If the descending time is shortened, it means that the malicious nodes are still present in the network.

In that case, the threshold should be adjusted upward. Otherwise, the threshold will be lowered.

Algorithm for Reactive defense phase

```
float threshold=0.9;
initialDefence();
float dynamic(threshold)
{           float t1,t2;
            t1=calculate the time of PDR down to threshold;
            if(PDR < threshold)
            initialDefence();
            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;
                        }
                        if(simulationTime < 800) {
                        return threshold;
                        dynamic(threshold);
                        }
                        else return 0.9;
}
```

The operations of the CBDS are captured in Fig. 4.3. It should be noticed that the CBDS offers the possibility to obtain the dubious path information of malicious nodes as well as that of trusted nodes; thereby, it can identify the trusted zone by simply looking at the malicious nodes reply to every RREP.

In addition, the CBDS is capable of observing whether a malicious node would drop the packets or not.

As a result, the proportion of dropped packets is disregarded, and malicious nodes launching a grayhole attack would be detected by the CBDS the same way as those launching blackhole attacks are detected.

DOI 10.17148/IJARCCE.2015.4426

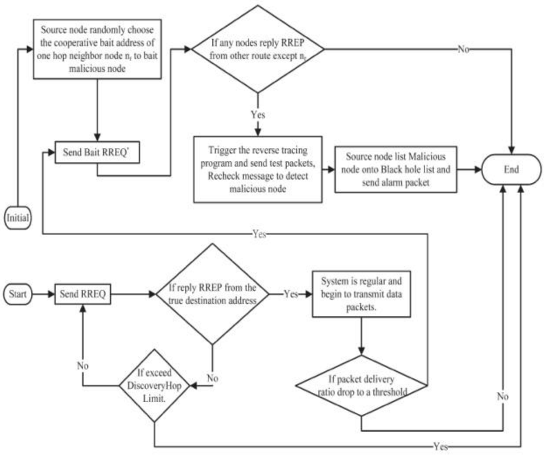
Initial
Source node randomly choose the cooperative bait address of one hop neighbor node n_r to bait malicious node
Send Bait RREQ'
If any nodes reply RREP from other route except n_r
No
Yes
Trigger the reverse tracing program and send test packets, Recheck message to detect malicious node
Source node list Malicious node onto Black hole list and send alarm packet
End
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

Figure 4.3: Operations of CBDS

III. CONCLUSION

In this approach, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative blackhole attacks. The address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list.

Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defense architectures to achieve the aforementioned goal.

REFERENCES

[1]. 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," Wireless Commun., VITAE, Chenai, India, 2011.

[2]. D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput,1996.

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

[4]. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003.

[5]. H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007.

[6]. 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.

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

DOI 10.17148/IJARCCE.2015.4426