International Journal of Electrical Electronics & Computer Science Engineering
Volume 3, Issue 1 (February, 2016) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

Preventing Attacks By Malicious Nodes In Mobile Ad-Hoc Network Using Dynamic Threshold Algorithm

Kavita Surve[1], Neha Jagadale[2], Pratiksha Kanadi[3], Manisha Changule[4]
[1-3]UG Scholar, Computer Science & Engineering Department, SRTTC College of Engineering, Pune, India
[4]Assistant Professor, Computer Science & Engineering Department, SRTTC College of Engineering, Pune, India
[1]kavitasurve999@gmail.com, [2]nehajagdale@gmail.com, [3]kanadipratiksha1995@.gmail.com, [4]manisha.changule@srttc.ac.in

Abstract: ***Today there is more and more popularity and usage of wireless networks .A mobile ad hoc network is the cluster of wireless mobile nodes that form a dynamic network without the infrastructure or base points. Mobile Means Movable and Ad-Hoc Means Temporary available. The dynamic nature of ad hoc networks introduces many security problems. Secure routing is the attractive area for achieving better safety for the network. Protecting the network can be done by using routing protocols from malicious attacks. There are many secure routing protocols had been proposed in the literatures that were successful in protecting and preventing security attacks in MANETs. MANETs are still unprotected to many types of attacks. Hence, there will be need for an efficient mechanism to search attacks by malicious nodes. Here this paper find a solution to this issue by proposing a dynamic source routing (DSR)-based routing mechanism ,which is referred to as the cooperative bait detection scheme (CBDS), that takes the advantages of both proactive and reactive mechanism.***

Keywords: DSR, CBDS, AODV, MANET, Black-Hole Attack, Gray-Hole Attack.

I. INTRODUCTION

A mobile ad hoc network (MANET) is infrastructure less network. A network which consists of many movable or mobile nodes communicating with each other's without any wired link between them is known as Mobile Ad-hoc network. In Manet single hop or multi hop modes are used by nodes for communication. In this network, each node not only acts as a host but also as a router.

An important task in mobile ad hoc network is the route discovery process, in which a path from a fixed source to a specific destination is discovered in order to transfer data packets via this identified route[1].Because of the dynamic nature of MANET topology and infrastructure less network they are more vulnerable to attack. Therefore the trust relationship amongst node may get disturbed. Also the detection of malicious node in network becomes difficult due to lack of base stations and traffic control in dynamic large scale network become complex. In literature many routing protocols have been proposed such as AODV and DSR for route discovery process.

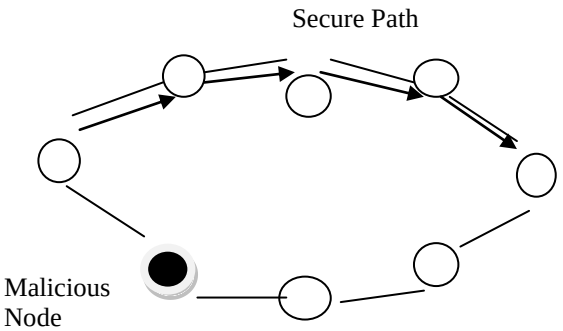

Fig 1 Mobile Ad-Hoc Network.

II. EXISTING SYSTEM

To provide security to the network and for detecting malicious nodes many techniques are available. For safe data transmission and communication number of routing protocols was used in literature survey. Routing protocol such as AODV (Ad-hoc On Demand Vector) and DSR (Dynamic Source Routing) protocols provides security by finding harmful nodes in MANET. Ad-hoc On demand Vector and Dynamic Source Routing protocols are the examples of reactive or source initiative protocols. To only detect malicious nodes in network these protocols are used and two ACK, BFTR techniques proposed in [4],[5] are used as benchmark scheme for performance checking purpose.

AODV allows mobile computers to pass messages through their neighbours to nodes with which they cannot directly communicate also it is able to handle changes in route and create new route if error exists. Dynamic source routing algorithm contains two main processes: 1.route discovery and 2.route maintenance. By using RREQ and RREP it communicates with destination. Here, RREQ means Route Request and RREP means Route Reply.

For the detection of routing misbehaviour in MANETs Liu et al. proposed a 2ack scheme [4]. 2ack scheme means two hop acknowledgment packets are sent to source node to confirm that data packets are received successfully. This scheme as it is belongs to proactive mechanism produces additional routing overhead despite of harmful nodes in network. Best effort fault tolerant routing scheme is proposed by Xue and Nahrstedt [5], known as prevention mechanism. Here end-to-end acknowledgements are used to monitor the

International Journal of Electrical Electronics & Computer Science Engineering
Volume 3, Issue 1 (February, 2016) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

quality of routing path which is chosen by destination node. But the drawback of BFTR scheme is malicious nodes may still exists in new path so repeated path discovery process is needed which leads to routing overhead.In this paper we are using CBDS (Co-Operative Bait Detection Scheme). CBDS is DSR-based routing protocol, it can identify all the addresses of nodes in the selected routing path from a source node to destination node after the source has received the RREP message.

III. PROPOSED SYSTEM

To detect grey hole/ collaborative black hole attacks in MANETs our proposed detection mechanism takes advantage of the characteristics of both the reactive and proactive schemes to design a DSR-based routing scheme known as co-operative bait detection scheme. There are many types of attacks in Manet one of the special type is black hole attack that generally occurs in reactive protocols. In this black hole attack, the affected node is falsely claiming that it has shortest and new path to reach the destination and attracts the data packet then drops the packet. Various harmful actions are performed by black hole node as follows:

- By falsifying the Route Request packet it act as source node.
- By falsifying the Route Reply packet it act as destination node.

Grey hole attack is variant of black hole attack. In this attack malicious node accepts data packets and drops some of them or changes the data packets and forwards it to destination. To reduce the resource wastage, our CBDS scheme uses the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps. In this paper we are maintaining security by using or implementing three steps:

A. Initial Bait Step

B. Reverse Tracing

C. Dynamic Threshold Algorithm.

Here first and second steps are proactive defence while third step is under reactive defence architecture.

A. Initial Bait Step:

In this first step, source node broadcast RREQ msg to detect or attract the malicious node. Then the neighbour node will reply to source node if node doesn't send reply or ACK msg to source node then source node will put that node in malicious list node. The goal of this phase is to attract 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 holds 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., nr, within its one-hop neighbourhood 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 Figure2. If nr deliberately gave no reply RREP, it would be directly listed on the black hole list by the source node. If only the nr node had sent a reply RREP, it would mean that there was no other malicious node in the network, except the route that nr 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.

Table I

PACKET FORMAT OF RREQ′

Option Type	Opt Data Len	Request ID
Target Address (RREQ' : Bait address)		
Address[1]		
Address[2]		
.....		
Address[n]		

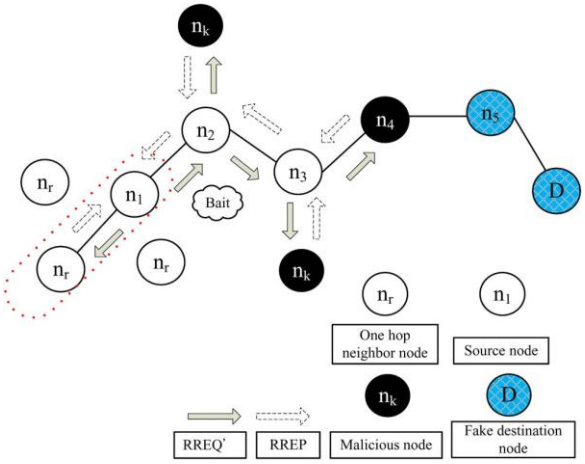

Fig. 2 Random Selection Of A Cooperative Bait Address.

B. Reverse Tracing:

The reverse tracing step is used to detect the behaviours 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. Testing or Dummy packets are sent in this step.

C. Dynamic Threshold Algorithm:

Here in this step threshold is set based on network efficiency between 80 %to 90%. Then according to

International Journal of Electrical Electronics & Computer Science Engineering
Volume 3, Issue 1 (February, 2016) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

threshold value and timing value this step detects the malicious node and put it into black list or malicious list.

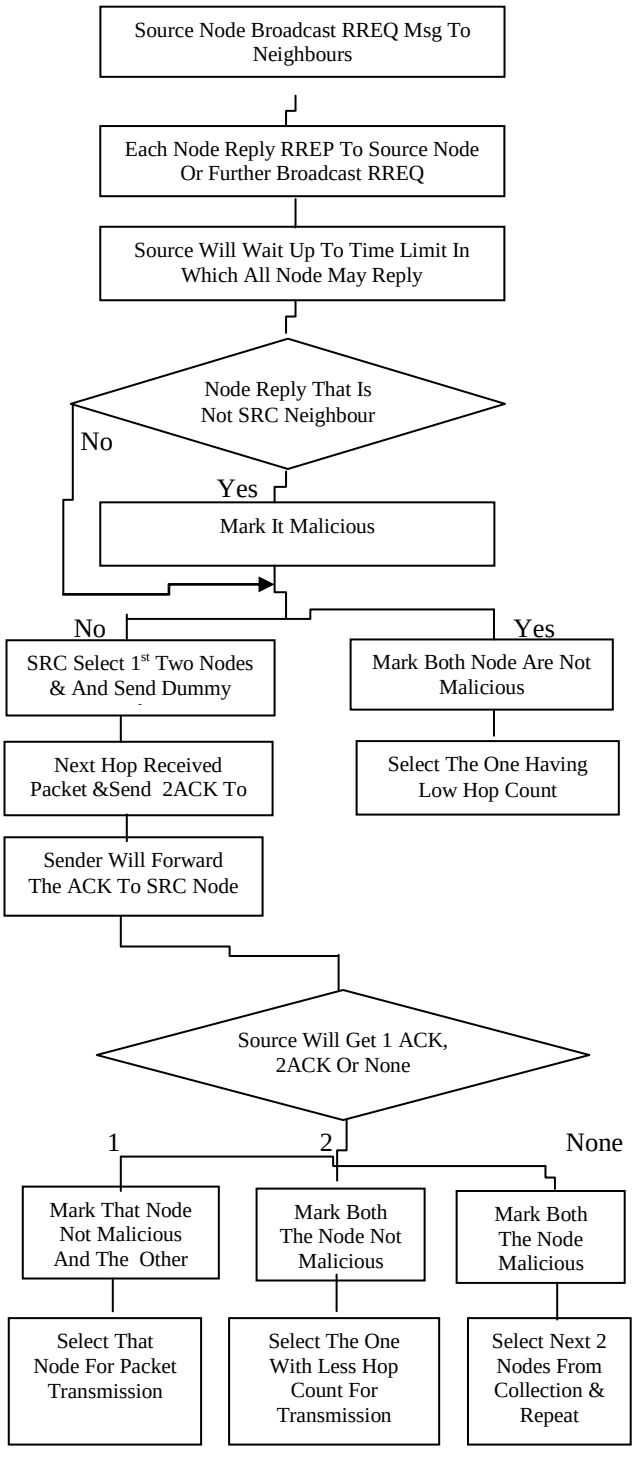

Fig. 3 Reverse Tracing Phase

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 initial threshold value is set to 90%. a dynamic threshold algorithm is designed 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 Dynamic Threshold:

```
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;
}
```

IV. CONCLUSION

In this project, we have proposed a new mechanism co-operative bait detection approach (called the CBDS) for detecting malicious nodes in MANET's under gray/collaborative black hole attacks. Our results revealed that the CBDS outperforms the DSR, 2ACK, and BFTR schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio

V. REFERENCES

[1] Yaser khamayseh, Ruba Al-Salah, Muneer Bani Yassein Jordan University of Science and

Technology, Dept of Computer Science Irbid, 22110, Malicious Nodes Detection in MANETs: Behavioral Analysis Approach, Vol. 7, No. 1, January 2012.

[2] Mrs. A. Naveena, Dr. K. Rama Linga Reddy, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 4, April 2015.

[3] M. Ahmer Usmani, Manjusha Deshmukh, Defending Against Attacks in MANETs using Cooperative Bait Detection Approach, Vol. 4, Issue 4, April 2015

[4] 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, pp. 536–550, May 2007.

[5] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Pers. Commun., vol. 29,pp.367-388,2004, April 2015.