Identifying and Preventing Attacks in MANETs Using Cooperative Bait Detection Scheme

SyedaMisba[1] ,Anusha H.M [2],Apoorva S[2],HemalathaS[2],Lakshmipriya N.P[2]

[1]Assistant Professor,[2]Student ,Information Science and Engineering

Vidyavardhaka college of Engineering, Mysuru

Affiliated to VTU belgaum, india

Abstract:The initial need to setup the communication of nodes in mobile adhoc network [MANETs] is that all the nodes should act together..In the Manets environment if any malevolent nodes are present in the obligation it may escort to grave attacks such as Black Hole and Grey Hole attack. Such nodes may Disrupt the Routing Process. Identifying and Prventing of attacks like Black Hole or the Gray Hole attack in network communication is the main challenge. In this context our paper is attempt to identify and preventing the malicious node using Cooperative bait Detection Scheme [CBDS] approach which is Dynamic source routing based [DSR] mechanism and place them into the black hole list and broadcast the alert message over the network. CBDS approach combines the benifit of both Proactive and Reactive Defence mechanism.

Keywords:- *Mobileadhoc network[MANETs], CBDS, DSR, Malevolent nodes, Black hole attack, Grey hole attack.*

I. INTRODUCTION

A mobile ad hoc network **[**MANET] is acontinously self constructing, substructure-less network with autonomous mobile nodes connected dynamically in an arbitrary manner through wireless links[1].These self governing nodes can communicate with each other if and only if they are in transmission range. As adhoc network is economically beneficial, it is being used in the many applications like collective and distributive computing, emergency services, wireless mesh and sensor networks and even in hybrid networks. Inspite of all these advantages MANETs have associated with some of the challenges. The major challenge in the MANETs is the secure communication. The mobile nodes by means of less protection are susceptible to attacks, The intruder can alter and stab to masquerade all the gridlock on the cellular communication channel as one of the authentic node in the network[3] .In the point of defenceelucidationstagnant arrangement might not be sufficient for the dynamically varying toplogy. In a MANETs, every particular node worksmutually as host and also as arouter. while data receiving cooperation is required with every other nodes to forth the packets, thereby it forms a wireless LAN.

These important features is also have some severe hindrance from security view point. The deficiency of any framework with the vibrant topology trait of MANETs made these networks extremely defenceless to network intrusion such as black hole and grey hole. Black hole attack in manets is a sober security issue to be clarified .In this attack a malevolent node make use of routing protocol to publicize itself that it has the shortest path to that node whose packet it desires to divert. Based on flooding protocol if any malicious node’s respond reach the requisition node before the actual node gives reply, a fake route has been formed. This malicious node can then decide whether to slump the packets or to utilize its position on the route. Grey hole is an attack that can change from behaving original to sinkhole, because it can act as normal node change over to malicious node, it becomes too typical to identify the state whether it is a normal node or malicious node[2].In this attack selective sinking of packets appears, and the information cannot be further transmitted. This paper attempting to identify the appropriate solutions to prevent the network from black hole and grey hole attacks.

Fig 1 shows how the black hole attack occurs is a source node that broadcasts route request[RREQ] packets to the nodes next to it in order to find the destination, they in turn sends packets to its adjacent nodes. The node D has to reply to the request and send the route reply[RREP] packet to the source through the adjacent nodes. The malicious node M reply with the false RREP claiming that it has a shortest path to the destination, attract all the packets by using route reply[RREP] packet then discards these packets without advance it to the actually destination.

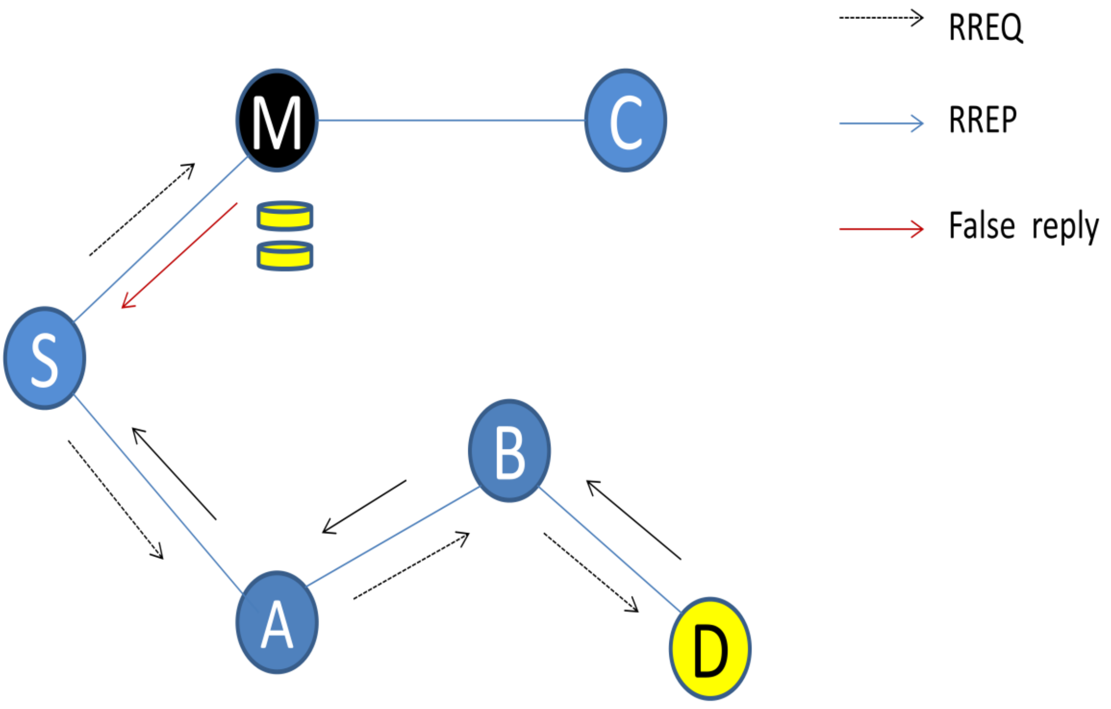


Fig-1 Blackhole attack

II. EXISTING SYSTEM

Dynamic source Routing includes mechanisms such as: route discovery and route maintenance. To launch the route discovery phase, the source node sends a RREQ packet over the network. If a neighbouring node has routing information to the target in its cache routing tablet replies with aRREP packet to the source node. When the route request (RREQ)packet is forecasted to the next hop, the node adds its address information into the route record in the RREQ packet[7]. When destination node gets the RREQ, it can identify each neighbouring node's address amongst the route. The destination node depends on composed routing details among the packets in order to send a reply RREP message to the basis node with the entire routing information of the found route.

A. Disadvantages of Existing System

- The insufficiency of any infrastructure added with the dynamic topology structure of MANETs make these networks highly exposed to routing intervention such as blackhole and gray hole.
- With respect to this context, the effectiveness of these approaches becomes weak and when malicious nodes are more in the network, they conspire together to start a collaborative attack, which may result to more damages to the network.

III. PROPOSED APPROACH

This paper introduces a detection scheme called the cooperative bait detection scheme[CBDS]whose objective is detecting and preventing malicious nodes launching grey hole/collaborative Black- hole attacks in MANETs. In our approach, the source node randomly selects a neighbour node with which to co-operate, in the sense that the address of this node is used as bait destination address to entice malicious nodes to transmit a RREP message. malevolent nodes are thereby detected and prevented from involving in the routing operation using a technique called reverse tracing ,in this technique it is assume that when a momentous drop occurs in the packet delivery ratio, an alarm is send by the target node back to the basis node to triggre the discovery mechanism again. our CBDS scheme combines the benefit of proactive detection in the initial step and the lead of reactive response at the subsequent steps in order to reduce the resource wastage.

Our CBDS method implements a reverse tracing technique to help in achieving the stated goal.

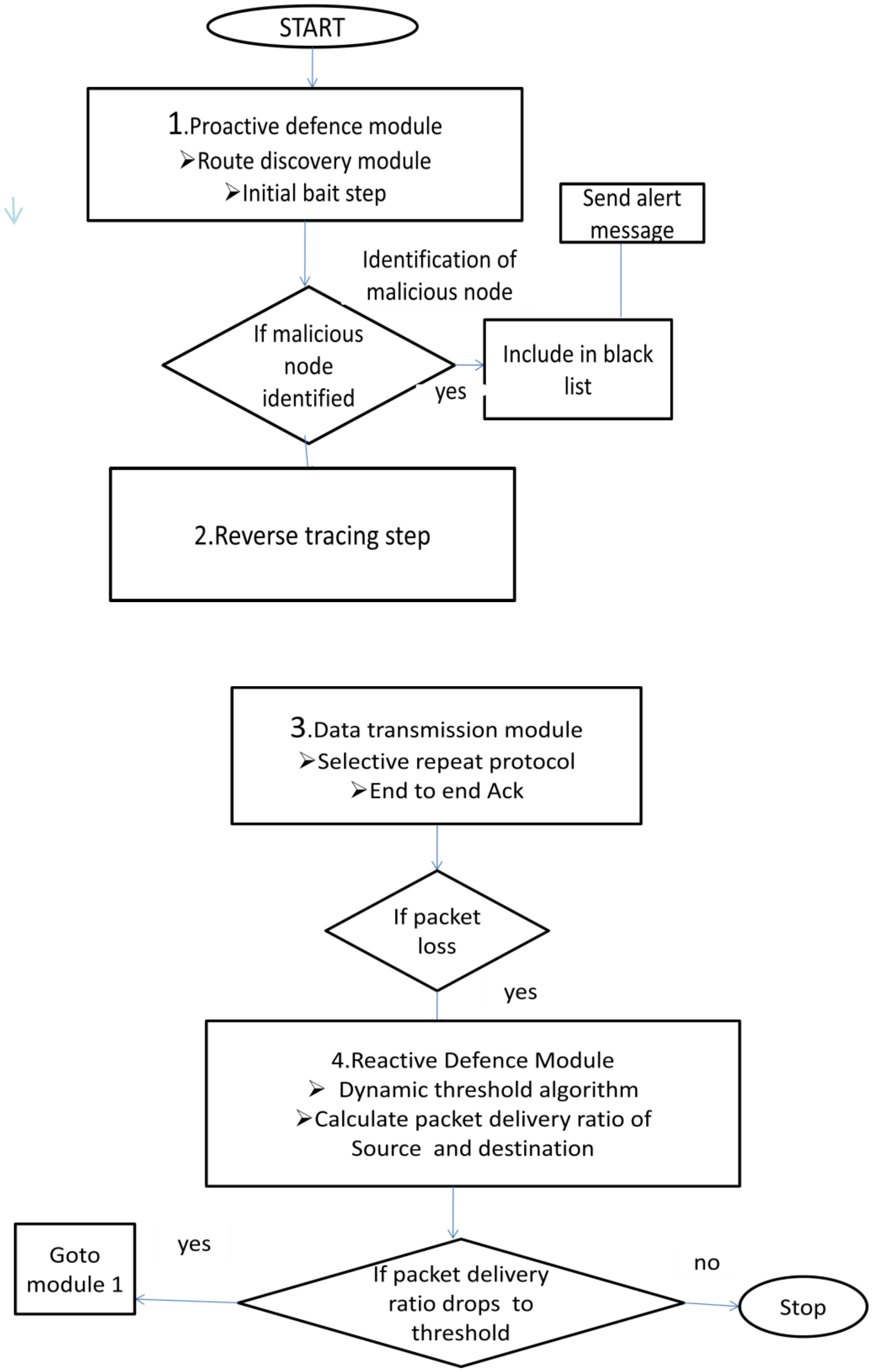
1 Initial entice step

2 The reverse tracing

3 Shifted to reactive defence

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

IV. OVERVIEW OF SYSTEM


START
1.Proactive defence module
➢Route discovery module
➢Initial bait step
Send alert message
Identification of malicious node
If malicious node identified
yes
Include in black list
2.Reverse tracing step
3.Data transmission module
➢Selective repeat protocol
➢End to end Ack
If packet loss
yes
4.Reactive Defence Module
➢ Dynamic threshold algorithm
➢Calculate packet delivery ratio of Source and destination
Goto module 1
yes
If packet delivery ratio drops to threshold
no
Stop

- Proactive Defence Module(UDP,Flooding method)

  - initial entice step
  - route discovery module

- ➢ Reverse tracing step
- ➢ Data transmission module
  - selective repeat protocol
  - End to end acknowledgement
- ➢ shifted to Reactive defence step module
  - Dynamic Threshold Algorithm
  - packet Delivery Ratio

A. Proactive Defence module

The initial proactive defence module is initiated inorder to check the network Behaviour before flooding the packets. this can be achieved by triggering the initial Bait step and the Reverse tracing step i.e given below

i. Initial bait/entice Step

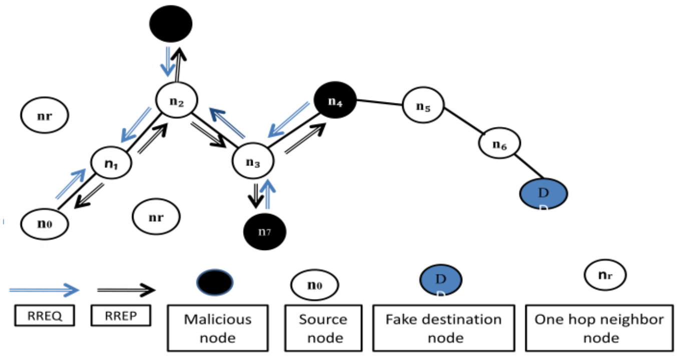


Fig 2. Initial Bait step

The objective of this stage is to attract a malicious node to send a reply RREP packet by sending the bait. to upgrade itself RREQ is used at very moment most shortest way to the node that enclose the packets that were modified over. In order to accomplish this objective the destination location of the bait RREQ is intended to create by accompanying the system. The source node automatically selects the neighbour node within its one hop and to work with this node as destination by using its address as bait RREQ.as each baiting is done randomly and if the node moved then the adjacent node would be changed, the bait would be changed. This is shown in Fig. 2.

A slight possibility that if $n_0$gave answer RREP intentionally and it is simply recorded on the black hole list by the source node. If the node n_0 send a reply RREP,it would intend that there was no other further malicious node in the network, apart from the route that REP had sustained; in this case,the phase of route discovery phase will be initiated. The scheme that n_0 attempts would not be archived in the result given to the phase of route discovery.

ii. Route Discovery Module

This module make use of Dynamic source routing protocol is a intelligible and efficient routing protocol devised especially to make use in mobile nodes of wireless ad hoc networks.DSR concede the network to be self-adapting and configuring, without making use of extant network framework. It has been enforced by several groups and extended on distinct testing structure. This protocol composed of two major technique: Route discovery and Route maintenance which work collectively to concede nodes to discovery and maintain routes to approximate destination in ad hoc networks.

To achieve the route discovery phase, the source node advertise a route request packet[RREQ] over the network. If an intervening node has routing information in its cache, then it reply to the source node with a RREP and then it is dispatched to the further nodes, that node will add it address details into the route field in the RREQ packet. when the RREQ request reaches destination node and can get to know all interposed node's address among the path and the destination depends on this poised routing information to transmit a reply RREP message to the source. This dynamic source routing protocol doesn't deal with any recognition technique, still the source node obtain the routing information regarding the nodes along the path we make use of this characteristic in our approach. In this paper, a system called co-operative bait detection scheme(CBDS) is conferred which detects the malicious node effectively that tryout to cast blackhole or greyhole attacks.

B. Reverse Tracing Step

The Reverse tracing step is mainly used to find the behaviour of the malevolent nodes through route reply to the RREQ packet message. If RREQ message has been received by the malicious node, then false RREP message is replied by it. correspondingly the reverse tracing operation will be performed for nodes who receives the RREP. The objective of this step is to conclude the suspicious path information and ethereal trusted zone in the route.

C. Data Transmission Module

Proactive and Reverse tracing steps are mainly used to identify the malicious nodes and their behaviour. once if the network is found to be secure without any malicious nodes. The optimal path obtained from the route discovery module will be used to transmit the data packets from source to the actual destination. if the network contains any malicious node then packets will not reach the destination instead that malicious node will drop all the packets without forwarding to actual destination.

D. Reactive Defence Module

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 defensephase[5]

```
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;
```

V. CONCLUSION

In this paper, we have scrutinized the security instability by proposing a new method known as cooperative bait detection scheme for identifying the malevolent nodes and preventing the attacks like Black Hole and Grey Hole attacks in MANETs .To identify the malicious node we make use of address of the neighbour nodes as bait destination to send the reply message and the malevolent nodes are spotted by using reverse tracing technique. If any malicious nodes are recognized means they are conserved in a list called black hole list and alert message is broadcast to the other nodes in the network in order to stop disseminating with any other node in that list. In order to achieve this goal cbds approach has been adopted which combines the advantages of both proactive and reactive mechanism.

REFERENCES

[1]Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, IEEE “Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach” in proc IEEE journal, 2014, pp. 1–11.

[2] P.-C. Tsou, J.-M.Chang, H.-C.Chao, and J.-L. Chen, “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.

[3] 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, pp. 570–575.

[4] 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, pp. 28–32, 2010.

[5] International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 4, April 2015 Copyrightto IJRECDOI10.17148/IJARCCE.2015.4426 115 Defending Against Attacks in MANETs using Cooperative Bait Detection Approach M. Ahmer Usmani1, Manjusha Deshmukh2 Lecturer, Department of Computer Engineering.

[6] W. Kozma and L. Lazos, “REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,” in Proc.WiSec, 2009, pp. 103–110. Kejun

[7]An approach for defending against collaborative attacks by malicious nodes in MANETs Miss Ashwini S. Barote , Dr. P. M. Jawandhiya, 1PG Scholar, 2Principal 1Computer Scienceand Engineering Department, 1PLITMS, Buldana, India © 2016 IJEDR | Volume 4, Issue 3 | ISSN: 2321-9939.