International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 382 - 386

Preventing Collaborative Attack by Cooperative Bait Detection Approach

Tanmayee Deepakrao Buradkar
Electronics & Telecommunication Engineering
G.H. Raisoni College of Engineering & Management
Pune, India
tanmayeeburadkar244@gmail.com

Prof. Bharti D. Patil
Electronics & Telecommunication Engineering
G.H. Raisoni College of Engineering & Management
Pune, India
bharti.patil@raisoni.net

***Abstract*—** Mobile Ad-hoc Network (MANET) falls in the class of remote impromptu system, and is a self-arranging system. Every gadget is allowed to move autonomously in any course, and henceforth will change its connection with different gadgets as often as possible. Every hub must forward movement which is not identified with its own particular use, and in this manner be both a switch and a recipient. This element likewise accompanies a genuine disadvantage from the security perspective. Within the sight of pernicious nodes, this necessity may lead genuine security worries; for occurrence, such node may irritate the directing procedure. In this connection, forestalling or distinguishing noxious nodes dispatching grayhole or collaborative black hole in test. This anticipate endeavors to decide this issue by planning a dynamic source routing (DSR)- based routing mechnism, which is alluded to as the Cooperative Bait Detection System(CBDS), that organizes the upsides of both proactive and receptive safeguard structures. This paper proposes a recognition plan called the Cooperative Bait Detection System (CBDS), which goes for distinguishing and counteracting noxious nodes propelling grayhole/Collaborative blackhole assaults in MANETs.

Keywords- *Cooperative Bait Detection Scheme (CBDS), dynamic source routing (DSR), collaborative blackhole attacks, mobile ad hoc network (MANET)*

*****

I. INTRODUCTION

In Mobile Ad-hoc Network (MANETs), a crucial necessity for the establishment of correspondence among nodes is that nodes ought to organize with each other. Within the sight of pernicious nodes, this prerequisite may lead genuine security worries; for occasion, such nodes may exasperate the directing procedure. Our CBDS framework executes an opposite following procedure to help in accomplishing the expressed objective. Reproduction results are given, demonstrating that within the sight of malevolent hub assaults, the CBDS outflanks the DSR, 2ACK, and best-exertion flaw tolerant steering (BFTR) conventions (picked as benchmarks) as far as bundle conveyance proportion and directing overhead (picked as execution measurements).

In a MANET, every node fills in as a host as well as go about as a switch. While accepting information, nodes additionally require collaboration with each other to forward the information parcels, in this way framing a remote neighborhood. These awesome elements additionally accompany genuine disadvantages from a security perspective. For sure, the previously stated applications force some stringent requirements on the security of the system topology, directing, and information movement. For example, the nearness and cooperation of noxious hubs in the system may disturb the steering procedure, prompting a breaking down of the system operations.

II. AIM AND OBJECTIVES

A. Problem Definition

This paper attempts to resolve the issues like Preventing or detecting malicious nodes launching grayhole or collaborative blackhole attacks in MANET's networks. In this our project design 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 defence architectures.

B. Objectives

i) **Packet Delivery Ratio:** It is defined as the ratio of the number of the number of packets sent by the source to the packets received at the destination.

ii) **Routing Overhead:** This metric represents the ratio of the amount of direction finding related control packet transmissions to the amount of data transmissions.

iii) **Average End-to-End Delay**: It is well-defined as the average time taken for a packet to be transmitted from the source to the destination.

iv) **Throughput**: It is defined as the total amount of data, that the destination receives them from the source which is divided by the time it takes for the destination to get the final packet.

III. OVERVIEW

In implementation phase of project implemented various module required of successfully getting expected outcome at the different module levels.

This phase is complete when all of the requirements have been met and when the result corresponds to the design.

A. Network Model

It consider a thick multihop static remote portable system conveyed in the detecting field, it accept that every hub has a lot of neighbors. At the point when a hub has parcels to send to the destination, it dispatches the on-interest course revelation to discover a course if there is not a late course to a destination and the MAC layer gives the connection quality estimation administration.

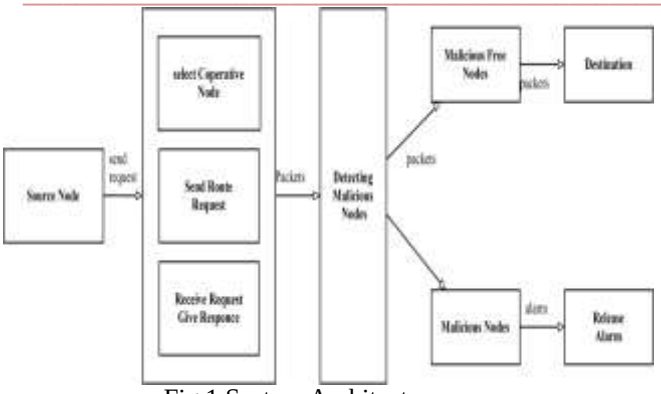

Fig 1 System Architecture

B. Initial Bait

The objective of the bait stage is to allure a vindictive node to send an answer RREP by sending the bait RREQ that it has used to promote itself as having the most limited way to the node that keeps the parcels that were changed over.

C. Initial Reverse Tracing

The converse following project is utilized to recognize the practices of noxious nodes through the course answer to the RREQ message. On the off chance that a malevolent node has received the RREQ, it will answer with a false RREP. As needs be, the converse following operation will be led for nodes.

D. Shifted to reactive phase defence

At the point when the course is built up and if at the destination it is found that the bundle conveyance proportion altogether tumbles to the limit, the discovery plan would be activated again to distinguish for constant upkeep and continuous response productivity.

E. Security Model

It will utilize the as key estimation of the message which will be sent and after that it is included with the general population key and sent from the source to destination through the middle of the road node afterward unscrambled in the destination by subtracting the public key from the message acquired and afterward the first message is gotten from the packets sent.

IV. ALGORITHM AND FLOW CHART

Algorithm considered here is in two steps as described below –

- **Algorithm for Reactive defence 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;
  }
```

- **Algorithm for Dynamic threshold**

```
double threshold=0.9;
  InitialProactiveDefence();
  double Dynamic (threshold)
  { double T1,T2;
        T1=Calculate time of PDR down to
threshold;
        if(PDR< threshold)
    InitialProactiveDefence();
  T2=Calculate the time of PDR down to threshold;
        If(T1<T2){
              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;
        }
```

A. Flow chart

As per the designing of the Whole system the flow chart can be formulated.

The flow chart considered for the describing is given as follows-

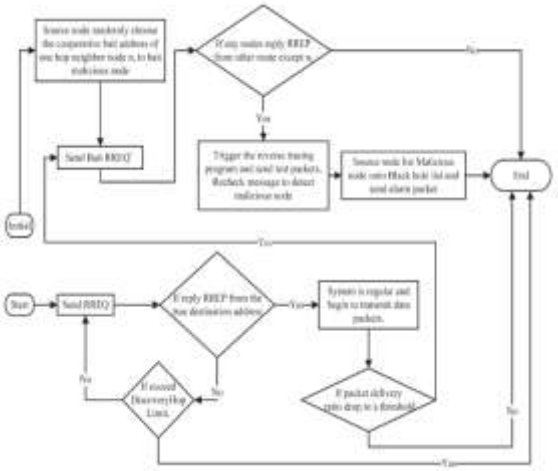

Fig 2 Flow Chart of Whole System

V. MATHEMATICAL MODEL

Let 'W' be the set of whole system which contains,
W= {RREP, RREQ', P, T, S,K,K' }.
Where,

1. RREP = Reply message.
2. RREQ' = message sent when attack occurred at some node.
3. P is the set of number of nodes in the network.
   P = {n1,…….nk,……nm,…..nr}.
4. T is set ot trusted nodes.If node nk receives the RREP, it will separate the P list by the destination address n1 of the RREP in the IP field and get the address list,

Kk = {n1, . . . nk}.
Where Kk represents the route information from source node n1 to destination node nk.
Then, node nk will determine the differences between the address list
P = {n1, . . . nk, . . . nm, . . . nr} recorded in the RREP and Kk = {n1, . . . nk}.

Consequently, we get

$$K'_k = P - K_k = \{n_{k+1}, \dots \dots n_m, \dots \dots, n_r\}$$

Where K'_k represents the route information to the destination node (recorded after node nk).

The operation result of K'_k is stored in the RREP's "Reserved field" and then reverted to the source node, which would receive the RREP and the address list K'_k of the nodes that received the RREP.
To avoid interference by malicious nodes and to ensure that K'_k does not come from malicious nodes, if node nk received the RREP, it will compare the following things:

1) A. the source address in the IP fields of the RREP;
2) B. the next hop of nk in the P = {n1, . . . nk, . . . nm, . . . nr};
3) C. one hop of nk.

If A is not the same with B and C, then the received K'_k can perform a forward back. Otherwise, nk should just forward back the K'_k that was produced by itself.
Suppose, we assume that node n4 can reply with K'_4 = {n5, n6}, n3 will check and then remove K'_4 when it receives the RREP.
After the source node obtains the intersection set of K'_k, the dubious path information S replied by malicious nodes could be detected, i.e.,

$$S = K'_1 \cap K'_2 \cap K'_3 \dots . \cap K'_k .$$

If malicious node would reply the RREP to every RREQ, nodes that are present in a route before this action happened are assumed to be trusted. The set difference operation of P and S is conducted to acquire a temporarily trusted set T, i.e.,

T = P – S.

If a single malicious node n4 exist in the route, the source node n1 pretends to send a packet to the destination node n6. After n1 sends the RREQ_, node n4 replies with a false RREP along with the address list,
P = {n1, n2, n3, n4, n5, n6}.
Here, node n5 is a random node filled in by n4.
If n3 had receive the replied RREP by n4, it would separate the P list by the destination address n1 of the RREP in the IP field and get the address list
K3 = {n1, n2, n3}.

It would then conduct the set difference operation between the address lists,
P andK3 = {n1, n2, n3} to acquire

$K'_3 = P - K_3$ = {n4, n5, n6}, and would reply with the K'_3 and RREP to the source node n1 according to the routing information in P.
Likewise, n2 and n1 would perform the same operation after receiving the RREP; will obtain

K'_2 = {n3, n4, n5, n6} and

K'_1 = {n2, n3, n4, n5, n6}, respectively;

and then will send them back to the source node for intersection i.e. ,
$S = K'_1 \cap K'_2 \cap K'_3$ = {n4, n5, n6},

This is the dubious path information of the malicious node.

Now to calculate the source node, P − S = T = {n1, n2, n3} to acquire a temporarily trusted set.

if there was a single malicious node n4 in the route, which responded with a false RREP and the address list,
P = {n1, n2, n3, n5, n4, n6}
then this node would have deliberately selected a false node n5 in the RREP address list to interfere with the follow-up operation of the source node.

However, the source node would have to intersect the received K'_k to obtain

$S = K'_1 \cap K'_2 \cap K'_3$ = {n5, n4, n6} and

T = P − S = {n1, n2, n3} and request n2 to listen to the node that n3 might send the packets to.

if n5 and n4 were cooperative malicious nodes, we would obtain
T =P − S = {n1, n2, n3}, and n2 would be requested to listen to which node n3 might send the packets.
Either n5 or n4 would be detected, and their cooperation stopped.
Hence, the remaining nodes would be baited and detected.

VI. SIMULATION RESULT

After tracing the shortest route and detecting the malicious nodes in the network, the parameters such as throughput, end-to-end delay, jitter, routing overheads, packet delivery ratio are calculated.

Fig 3,4,5,6,7,8,9,10 shows all the simulated results.

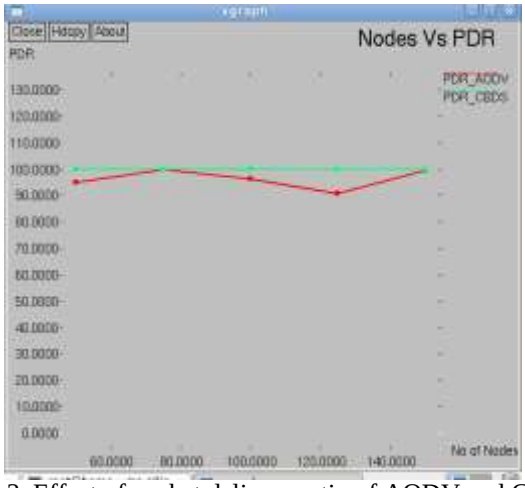

Fig 3 Effect of packet delivery ratio of AODV and CBDS

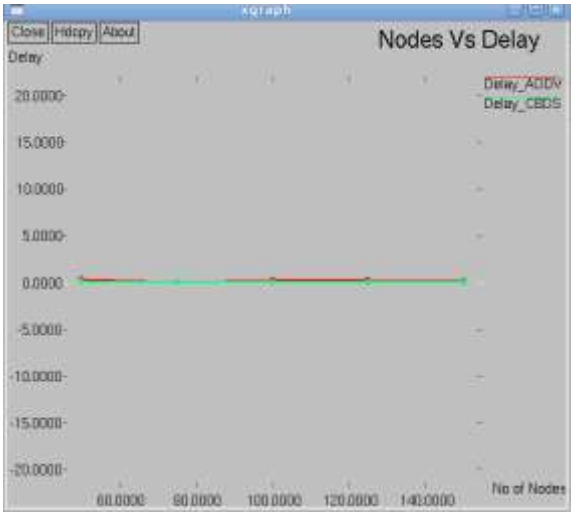

Fig 4 Effect of Delay of AODV and CBDS

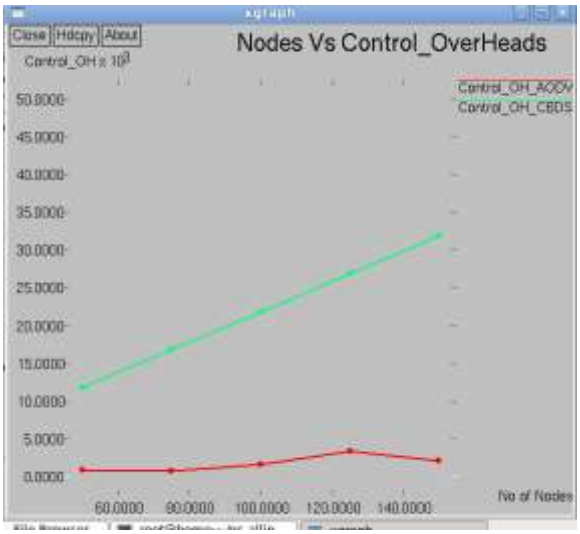

Fig 5 Effect of Control Overheads of AODV and CBDS

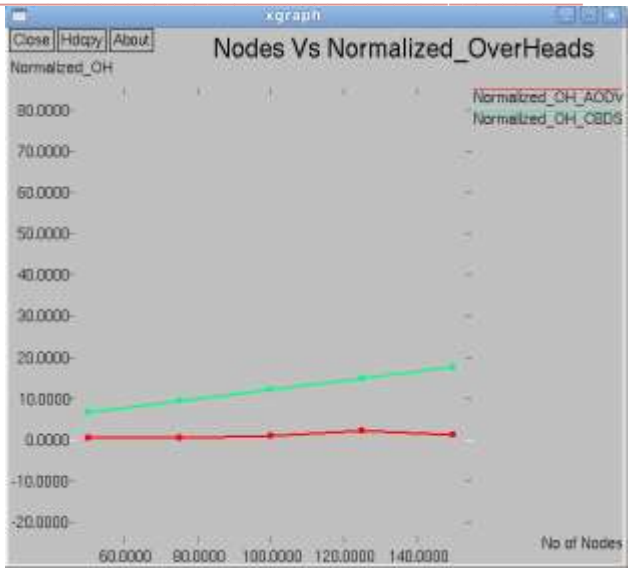

Fig 6 Effect of Normalised Overheads of AODV and CBDS

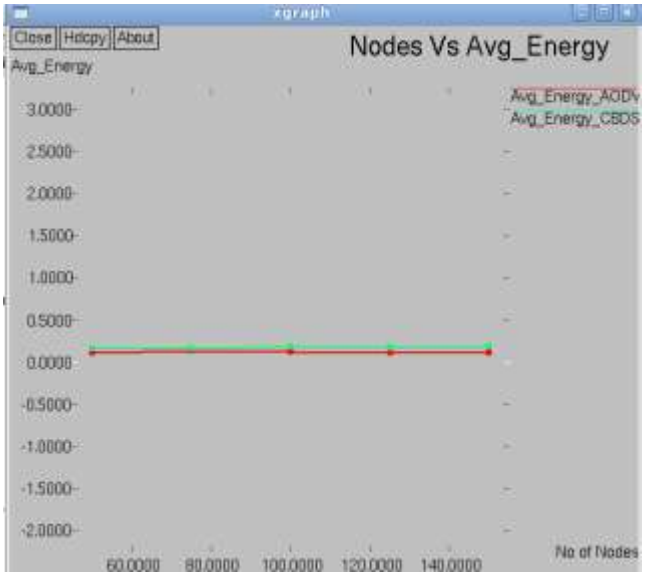

Fig 7 Effect of Average Energy of AODV and CBDS

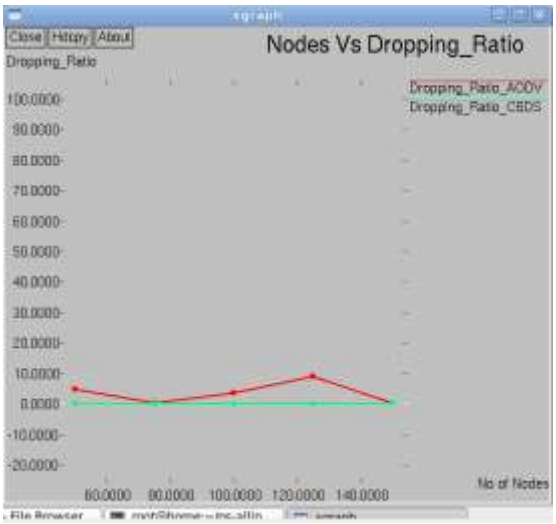

Fig 8 Effect of Dropping ratio of AODV and CBDS

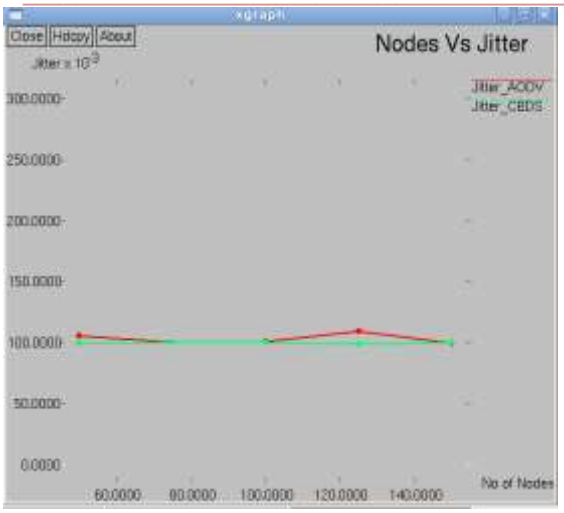

Fig 9 Effect of jitter of AODV and CBDS

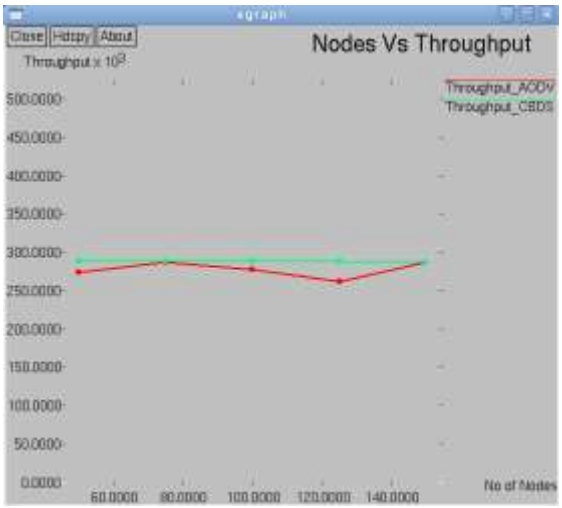

Fig 10 Effect of throughput of AODV and CBDS

CONCLUSION

In this methodology, we have proposed another instrument Cooperative Bait Detection Scheme (called the CBDS) for identifying malignant nodes in MANETs under dark/communitarian blackhole assaults. The location of a neighboring node is utilized as goad destination location to draw malevolent nodes to send an answer RREP message, and noxious nodes are distinguished utilizing an opposite following procedure. Any recognized malignant node is kept in a blackhole list so that every single other node that take part to the steering of the message are cautioned to quit speaking with any node in that rundown. Dissimilar to past works, the value of CBDS lies in the way that it coordinates the proactive and receptive safeguard designs to accomplish the previously stated objective.

1) inquire about the attainability of modifying our CBDS plan to manage other diverse sorts of communitarian assaults on MANETs and

2) inquire about the incorporation of the CBDS with other surely understood message security approaches in order to construct a complete secure steering system to ensure MANETs against bastards.

REFERENCES

[1] David B. Johnson and David A. Maltz *"Dynamic Source Routing in Ad Hoc Wireless Networks"* , Mobile computing, Kluwer Academic Publishers, 1996. Pittsburgh, PA 15213-3891.

[2] Hongmei Deng, Wei Li, and Dharma P. Agrawal *"Routing Security inWireless Ad Hoc Networks"* IEEE Communications Magazine , 0163-6804, October 2002.

[3] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" Department of Computer Science, IACC 258 ,Fargo ND 58105, 2002.

[4] William Kozma Jr. and Loukas Lazos " REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits" WiSec'09, March 16–18, 2009, Zurich.

[5] Raja Karpaga Brinda. R and Chandrasekar. P ***"****Defense Strategy for the Detection of Black Hole Attack in DSR"* An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Dec. 2011, Vol. 5.