Detection and Prevention of Selfish Node in MANET using Innovative Brain Mapping Function: Theoretical Model

Abhishek Gupta
TRUBA Institute of Engineering & Information Technology
Bhopal ,India

Amit Saxena
TRUBA Institute of Engineering & Information Technology
Bhopal ,India

ABSTRACT

Mobile ad hoc networks are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links without using an existing network infrastructure or centralized administration .As network is created on temporary basis that's why it is called adhoc network .In such network nodes have various limitation due to its adhoc nature. Hence resources like power , computing ability, battery are very precious in such type of networks. So some nodes decided not to cooperate with other nodes and simply aim to save its resources to the maximum while using the network to farward its own packet these type of node are called "Selfish Nodes" this problem is very common in adhoc network due to its configuration setup. In this paper ,we present a new mechanism that solves the problem of selfish node theoretically with the help of Innovative Brain Mapping function Model.

Keywords

Selfish Nodes; Mobile Ad-Hoc Networks (MANETs);Brain Mapping Function(BMN)

1. INTRODUCTION

Ad hoc networks consist of wireless nodes that self configure to form a network with no fixed infrastructure, they can be quickly set up as needed. Such nodes cooperate in routing to allow each node to communicate beyond its direct wireless transmission range [2].In such type of network nodes depend on each other for routing and forwarding packets. However, to save power and other resources, nodes belonging to independent authorities may behave selfishly, and may not be willing to help other nodes . A node may be able to communicate with other nodes far away with the cooperation of intermediate nodes, forwarding the packets to the destination. In this multi hop communication, each nodes operates as both host and router. Common routing protocol of Adhoc network such as DSR [3], AODV[4] have been designed to handle such environment.

Minimal configuration, quick deployment and the absence of central governing authority make MANET suitable for emergency situations such as natural disasters, military conflicts and emergency medical situations [4].However, since there is no centralized administration, the performance of a MANET greatly depends on the cooperation of all nodes in the network. In this paper, we propose a theoretical model to detect and prevent selfish nodes that refuse to cooperate but at the same time still use the network for their own benefits.Actually this model is also worked fine for any misbehaving node attack in adhoc network but in this paper the focus on selfish node.

This paper is organized as follows. In section 2,we briefly introduce existing solution of the selfish node detection. In section 3,we provide comparative study of methods those are already present for detection of selfish nodes, Section 4 gives overview of proposed model and the key assumption made in it. Section 5 illustrates Working of proposed model. Section 6 concludes this paper.

2. BACKGROUND

Two main schemes were proposed for selfishness overcoming, one which is reputation scheme and the other is price-based scheme. Reputation systems have the following main components: Monitoring unit, which observes the node's neighbor behavior, reputation unit which rates the neighboring nodes' behavior forming a reputation table, alarming unit which sends and receives alarms, and path manager which manage routing and forwarding decisions based on reputation values. Such components can be either implemented in every node or distributing among the system's nodes. Two reputation schemes were proposed in the literature, they are considered as the base stones for other suggested schemes. The first is CONFIDANT [6], where global reputation and alarm message were used to achieve the aim of reputation sharing. Therefore, it could learn others' experiment fully and punish misbehaving nodes. The second is CORE [7], which used a monitoring technique and reputation mechanism, where each node computes a reputation value for every neighbor using a reputation mechanism that differentiates between subjective, indirect and functional reputation. In this technique, the network's nodes refuse to provide service to the misbehaving node if its reputation is lower than a threshold, which can lead to be eliminated from the network. Bansal and Baker proposed an OCEAN [2] reputation scheme, where each node only saves one-hop neighbor's reputation, reputation updates couldn't be exchanged with each other and merely depend on subjective observation. In OCEAN misbehaving nodes have second chance to get service and adopt some measures to settle false accusation and inconsistent reputation value. On the other hand, price-based schemes provide mechanisms that encourage nodes to be well behaved. In such schemes, the concept of virtual cash was proposed, where nodes are rewarded for messages forwarding either through trading virtual cash with source and next hop nodes throughout the routing path to packet destination. In the price-based systems, Buttyan and Hubaux [8] introduced nuglets as credits for managing forwarding transactions. Two payment models, message purse model and message trade model, were proposed. In the former, a source node pays relay nodes by storing nuglets in the message head. Intermediate nodes acquire nuglets when forwarding the message. In the latter, a relay node buys messages from the previous node and sells them to the next

node in the path. The credit-based system in [5] uses credit clearance service and message receipts. When a node forwards a message, it keeps a receipt and uploads it to the credit clearance service for credits.

3. COMPARATIVE STUDY

Table – 1Comparative Study of Existing Methods for Detection of Selfish Nodes in Manet

sno	Credit-based System	Reputation-based System	Acknowledgement based system
1.	Based on Virtual Money Concept.	Based on Reputation metric for each node.	Based on Acknowledgement.
2.	Costly Security modules required for protecting the virtual money or nuglets	No such modules required.	No such modules required.
3.	Packet purse model(PPM),packe t trade model(PTM) are using credit based approaches.	Watchdog Model,Pathrater are using Reputation based approach.	Secure 2ACK Routing Protocol In MANET are using both i.e reputation plus acknowledgement approaches.

4. Overview of the Proposed Architecture

we made scheme on the real fact that everyone want to live and struggle for its existence if anyone is sure that he will not going to die because of deficiency of resources then it will be more chances that he will not cheat others for resources . The same concept is used in the core of proposed theoretical model. Assumptions in the model:

4.1

The Brain Mapping Function Node (BMFN):These node perform Brain Mapping functions for all nodes present in adhoc network.The important parts of Brain Mapping nodes are

1)***IDPS module*** **:**This Module has the capability of detection and prevention of selfish node.

2)***Turi machine*** **:**It comprises of infinite memory capability to store virtual node.

3)***Virtualization*** **Layer:** This Layer is used for creating virtual node.

IDPS MODULE WORKING ALGORITHM:

This Module works on the algorithm given below .In this first we define parameters that we used in our algorithm then we used three functions they are:

i) RREQ_B(S, D, rr)

ii) Selfish_Node ()

iii) Check_Selfishness (S,D,M)

```
Set mobile node = M          //Total Mobile Nodes
Set source node = S          //S Ɛ M
Set Destination Node = D     // D Ɛ M
Set Routing Protocol =AODV
Start simulation time = t0
Set radio range = rr;    //initialize radio range
```

I. RREQ_B(S, D, rr) // broadcast for communication and send request packet to D node

```
{
If ((rr<=250) && (next hop >0))
        {
        Compute route ()
                {
 rtable->insert(rtable->rt_nexthop); // nexthop to RREQ source
         if (dest==true)
{       send ack to source node with rtable;
Data_packet_send(s_no, nexthop, type)
                }
else            {
                destination not found;
                }
        }
        }
        else { destination un-reachable ;
   }
        }
```

II. Selfish_Node () //Selfish Node Work

```
        {
          Check (incoming packet)
                        { If (pkt == 'Routing')
                {Capture and updated destination field ;
                        Send route ACK to sender;
                                        }
Else if (pkt == 'TCP')
                        {Block TCP packet }
                        Else If {pkt =='UDP'}
                        {Capture UDP packet;
                 Can't Send to Destination;
                                        }
                        Else ( pkt =='other')
                        {Drop;    }
        Set     inf_pkt= (scan_rate * s_max_ / selfish node);  // infected packet send's to all normal node
```

```
Selfish_Broadcast (inf_pkt, nexthop)
                    {
          Set priority = 1       //Higher priority
          Send inf_pkt = 100 pkts/ms          //
greater than the limit
          Find (number of pkt accepted node)
                    }
```

IPS for Elimination of Selfishness Algorithm

```
Set IPS node = p ; // IPS node
Set routing =AODV ;
RREQ_B(p, n, rr)          // broadcast for communication
and send request packet toall n nodes via p node
          {
          If ((rr<=250) && (next hop >0))
                    {
          Set inf_rm = ( scan_rate *pkt s_max_ /
selfish node);  // infection disable module
                    If (inf_rm  => 100)
                              { Selfish Node Block ;
                    }
```

III. Check_Selfishness (S,D,M)

```
{
  If ((node € M) && (pkt < 100 pkts/ms)
     {
        pkt accepted by neighbor;
        pkt_Accept_limit();


     }
   Else { Node_Selfish()
          { can't accept by neighbor ;
            Block pkts sender ;
          }
        }

}
```

```
If  (any node belong is in radio range && receives that request
packet && heavy load node)
          {
Node l = week node          // l ϵ n
Check load of  Node l ;
If (load > normal load)
          {
          Inf_rm = 1;
          {
Node infection remove via inf_rm  parameter ;
          }
          }
                              }
                              Node unreachable;
                    }
                    Node out of range;
          }
```

5. Working of proposed model

The working of model is very simple the Brain Mapping Function Nodes(BMFN) are created in adhoc network the number of BMFN depends on factors like area, radio range strength, data importance etc.The BMFN is very robust and effective because it takes concepts of various fields like theory of computation(toc),neural network, artificial intelligence, and many more so it has advantages of all these fields. The structure of BMFN node is shown in fig 1(a)

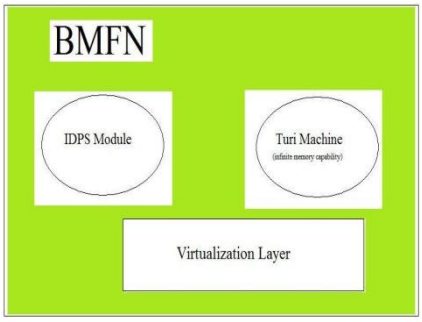

fig1(a):Architecture of BMFN Node

Fig1(a):Architecture of BMFN Node

This model is really unique because as we saw in previous literatures no model has given till today that incorporates advantages of so many fields in one model. Furthermore this is the first model that looked in new trends of technology like virtualization which gain popularity day by day instead of old conventional methods .In this method, whenever any node would be reached to the state of the power off , it immediately send signal to nearest BMFN node requesting for virtual node creation on hearing the request only the nearest BMFN node respond to that node .And saves the status plus all the information in its memory, there is no problem of memory capacity in it because model uses turi machine having infinite memory capability for this purpose. Then BMFN node creating virtual node in adhoc environment this is somewhat similar concept to have more than one operating system virtually onto a single operating system with the help of softwares like VMWARE ,ORACLE VIRTUAL BOX etc.This could be done by virtual layer for the model. Now when the same node previously exhausted(in terms of resource) come again(power-on)detected by BMFN node based on unique id information that stored in memory table of BMFN node, it immediately send this information to other BMFN node so that all the BMFN node deleted this information from its memory simultaneously. Before deleting virtual node the BMFN node

which detects the power-on occurrence of node resend all the data ,status information to the same node . During the period the node is power off all the information exchanged in that time period is up to date by BMFN node .So there is no problem of old and new information mismatch. But some nodes are greedy in nature means they know that they are not going to die even knowing the truth they behave selfishly this is analogous to real world situation in which some rich people have enough resources of living but even though they snatching resources from poor people only because of their nature or greed. For such types of nodes we have IDPS system in built in Brain Mapping Function Node that would take care of such type of nodes .Algorithm for it is already given in the section 4.1

6. CONCLUSIONS

In this paper, we propose a new scheme to detect and prevent selfish node furthermore it could be possible for some networks this scheme provide fully freedom from selfish nodes and increase throughput and performance that could not be achieved till yet. For our future work ,we planned to implement this theoretical model in to a fully working practical model .We also planned to decrease assumption as much as possible in this model so that in real test bed scenario this model works fine and smooth .We also would like to incorporate advantages of other fields in our models so that it would become more efficient, moreover we really try to generalize this model in such a way that it will works fine for any misbehaving node attack of adhoc network.

7. REFERENCES

[1] Bakar, K.A.A. A Scheme for Detecting Selfish Nodes in MANETs Using OMNET++, Wireless and Mobile Communications (ICWMC), 2010 6th International Conference ,pp. 410 - 414

[2] S. Bansal and M. Baker, "Observation-based Cooperation Enforcement in Ad Hoc Networks," 2003.

[3] J. Broch, D. B. Johnson, and D. A. Maltz, “The dynamic source routing protocol for mobile ad hoc network,” in IETF, February 2003, internetDraft Version 08.

[4] C. E. Perkins, E. M. Royer, and S. R. Das, “Ad hoc on-demand distance vector (aodv) routing (rfc3561),” in The Internet Society, 2003, memo RFC 3561

[5] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof,credit-based system for mobile ad-hoc networks," IEEE INFOCOM, 2003,pp. 1987-1997

[6] S. Buchegger and JY. Le Boudec, "Performance analysis of the CONFIDANT protocol," Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, 2002, pp. 226 -236

[7] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Advanced communications and multimedia security: IFIP TC61TC11Sixth Joint Working Conference on Communications and Multimedia Security, September 26-27,2002, Portoroz, Slovenia, 2002, p. 107.

[8] L. Buttyan and JP. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," Proceedings of the 1st ACM international symposiumon Mobile ad hoc networking & computing, 2000, pp. 87-96.

[9] E. M. Royer and C.-K. Toh, “A review of current routing protocols for ad-hoc mobile wireless network,” IEEE Personal Communications vol. 6, Apr 1999 ,pp. 46–55