ISSN (Print) : 2319-8613
ISSN (Online) : 0975-4024

Detection of Selfish and Malicious Node in Mobile Ad-Hoc Network with NS-2 Using Chord Algorithm

Sathya bama B [#1], Indira K [*2]
[#] Department of Information Technology, Sathyabama University
Chennai, Tamil Nadu, India
[1] sathyabama9392@gmail.com
[2] indira.it@sathyabamauniversity.ac.in

***Abstract*— In recent years Mobile Adhoc Network is developing as an important technology in wireless networks. It showing quick progress and has many applications. These types of networks provide strong and fast data delivery to users in wireless network. In WMN routers use advanced antennas to transmit data to each other in multi-hop manner. In MANET, it is easily to attacks because of dynamical changing of network topology, more centralized monitoring, management point and co-operative algorithm. The important fact in mobile adhoc network is security which being accepted by many people. The major problem of MANET is selfish node. Selfish nodes in MANET do not participate in forwarding packets. Due to Some misbehavior reasons a node can be identified as selfishness or malicious. Node selfishness may be a reason to which causes minimum delivery ratio of packet and data loss in the network. In MANET network, node failure is a reason for high end-to-end delay. In this paper we propose chord algorithm to overcome these issues, chord is structured peer-to-peer protocol. To provide P2P Nodes Service in Mobile Adhoc Network Chord is applied in MANET. The major advantage of Chord algorithm is greedy forwarding, aggressive update, passive bootstrapping and overlay broadcasting. Chord in MANET might be efficient, because it is not only providing direct routing but also provides indirect and key based of overlay routing. Our proposed system suggests that Chord technique can outperform in random routing in conventional way.**

Key words— MANET, Chord Algorithm, Greedy forwarding.

I. INTRODUCTION

Ad Hoc networks nodes forms network without any fixed infrastructure. Each node in adhoc networks is a self-configuring nodes and it acts as router and system [1]. In this type of environment, if one node wants to forward a data packet to destination node that node will be going to enlist other nodes in that network because of limited range of transmission [2]. Each node in adhoc network will not only acts a host but it also acts as router to transmit packets to other nodes in the adhoc network that may be within a range of direct transmission or not. In adhoc network, routing protocol allows nodes to find multi-hop paths to other node through that network. This type of idea gives fewer infrastructures in MANET networking, because each mobile nodes form their own routing in network themselves on fly. In adhoc network many routing protocols are designed based on only the assumption so that every node transmits every packet, but practically some of them acts as selfish, it means that nodes use network and service but it do not have interest to forward data packets to other nodes to save its resources and energy [3]. Malicious nodes attack is nodes misbehaviour has to bear some energy costs in order to perform the threat. In adhoc network selfish nodes do not have any interest to damage any other packet directly, but it is not interested to spend CPU cycles, battery life, or bandwidth of available network to transmit packets in direct transmission, it expects any others node to transmits packets. Selfish nodes in mobile adhoc network preserve its own resources when forwarding packets to others for consuming its resources. Identifying routes and transmitting packets to other node consumes CPU time, network-bandwidth, and memory [1].

Selfish nodes can be described in three ways depend on that attacking technique:

SN1: These types of nodes participate in discovering of route and maintenance of route phases but it is not willing to transmit data packets to save its own resources.

SN2: These types of nodes are not interested in the data forwarding and in route discovery and only participate to transmit their own packets.

SN3: These types of nodes behave correctly if their energy level lies between certain threshold of T1 and full energy-level of E. Selfish nodes behave as node type of SN2 if energy level lies between threshold of T1 and threshold of T2 and if level of energy comes under below T2 they behave as node type SN1[4].

Node isolation is a direct effect of node failures and misbehaviours in wireless adhoc network because nodes in wireless network communication depend on routing and packets forwarding.

In turn, selfish node presence is a direct reasons for network partitioning and node isolation, it further affects survivability of network and loss of data in the network and minimizes the delivery ratio of packet. Node failure is an important reason for end-to-end delay in adhoc network. To identify these issues and overcome, we use Chord Algorithm which is popular peer-to-peer protocol. The chord technique supports only one operation: gives key to node and maps that key into node. The key received node might be responsible for storing value or data associated to that key [5, 6].

II. RELATED WORKS

This section deals with the exiting solution of identifying and managing the selfish nodes in MANET network. Selfish nodes in network usually do not participate to forwarding packets to other node for saving its own resources. In MANET selfish nodes do not participates in packet transmits and routing. In CoCoWa method it finds selfish nodes with together local watchdog detections and send this information to other nodes. It sends selfish node detail to other node whenever contact occurs with other nodes. In MANET, nodes are vulnerable to many attacks like selfishness attack, Black hole, fabricated route, Resource consumption because of dynamic topology and lack of infrastructure [7]. In reputation based method path ratter and watchdog approach overhear of IDS neighbors' transmission of packet promiscuously and inform misbehaviour detail to source node by transmit messages. To escape form unreliable nodes in path finding source node gather notification and rates of other node. This method is easy to implement but it depend only on casual listening that give results of false identification. In scheme of CONFIDANT, the IDS execute task in distributed ways, the node in monitor casually observes the behaviour of route protocol and neighbor node packet transmission. Trust manager sends alarm type information on misbehaviour detection. In Reputation scheme: maintains a blacklist and a rating list of other nodes. The manager of path ranks a path according to nodes reputation besides each path. This system uses both indirect and direct observation from other node. In this system the opponent nodes are not removed from network but black listed. As Selfish node detection depends on other nodes that minimize the IDS reliability because the above mentioned nodes may give error result that may be blacklisted in non enemy node [8]. In credit based system node S sends Central Authorized Server (CAS) a receipt to each forward packet, then the Central Authorized Server provide credits to node depending upon the receipt. This scheme is useful because the implementation of this approach is easy but the main problem is message overhead and scalability. The author in [9] implements a method based on threshold in MANET. In this scheme, an effective and experiment approach was proposed by threshold value to identify selfish node. If node in MANET has equal and more than the threshold value of detected number of misbehaviour then that node will be noted as a selfish node. The author [10] proposed to implement the detection of selfish node and deletion. The objective of selfish node is to maximize benefit of its own. When the selfish node participates in process of routing it gets benefits. The selfish node in the network has different reasons to avoid packet transmission rather than sending packet

III.PROPOSED WORK

A.Overview of Proposed Work

Our main aim in proposed system is to find selfish node and malicious node in MANET using chord algorithm. The main operation of chord algorithm is assigning a key to node, and then it maps that key to that node. While mapping keys into the nodes, location services and traditional name provides direct mapping from keys to values. That value could be a document or an arbitrary item of data, or an address. Chord technique can easily put this functionality by each pair of key/value. Chord algorithm finds the selfish node when moving key from one node to other in the network and it also specifies how new node joining the system, how to identify location of the keys, and how to retrieve from failure of existing node.

B. Network Construction with Friend list add on system

Network Construction is first step to construct network with n no of nodes. So that nodes in the network request a other nodes to transmit the data packets from that node to other node. In this paper we create a multiple network, in which each network has n no of nodes. Network construction gives the benefit to nodes to transmit the packet in multiple ways. After successful network construction we use friend list add on system. In friend list add on system we use the node frame for keep the neighbor nodes information. Using that node frame nodes in that network can easily get details of neighbor nodes information. Every node in network has neighbor node details for path selection and communication purpose. Each node in network has friend list. So that transmission of data packet is achieved quickly and reliably.

C. Architecture

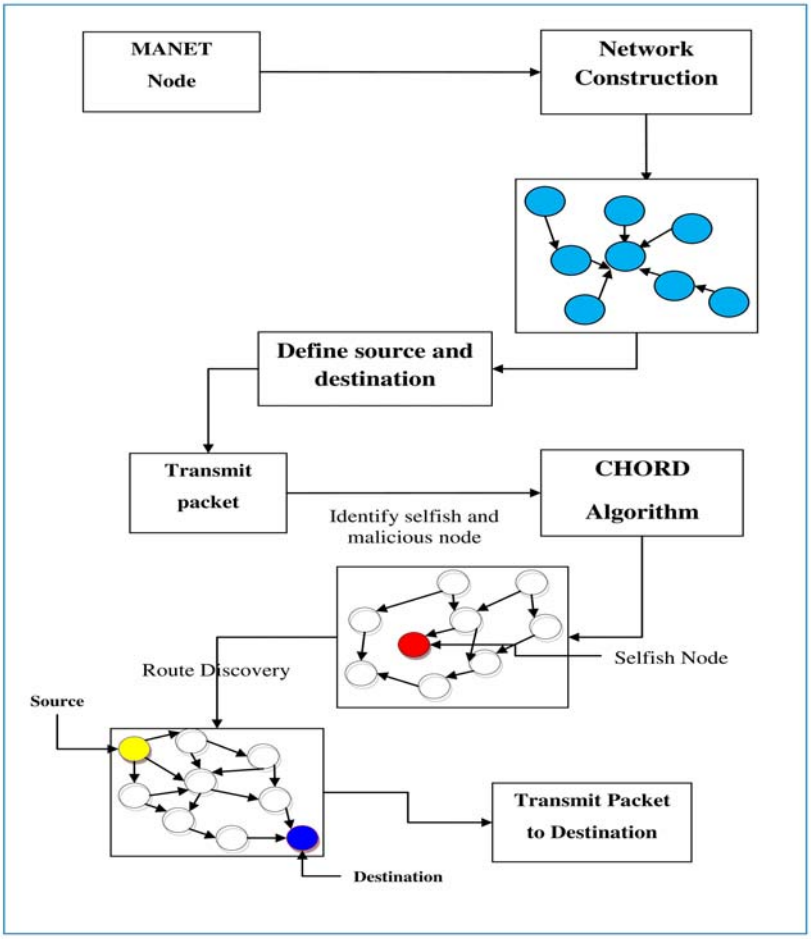

Fig. 1 Architecture

D. Identify the Selfish node using Chord technique

In our proposed scheme first group the nodes using network construction. Every node in the network will have information of neighbor nodes. In MANET, Network construction increased capacity of network and reduced overhead routing gives more effective and efficient routing in Mobile adhoc network. Usual routing protocols of adhoc network route a packet from source to destination using destination's address of node. In this paper we propose chord technique, chord technique assigns keys for each node in the Network group and sends that keys to neighbor node in the network group. Then nodes send a packet from source to destination using that chord key. Whenever a chord node in MANET gets an ID key, it will send that ID key to neighbor nodes in that network group. When forwarding that key to neighbor nodes if any intermediate nodes in that network do not like to move that key to other node then Key sender node in the network will identify that node is selfish node, then that Key sender node send that selfish node information to neighbor nodes in the friend list group and update that information in its node frame also. We use the watch dog activity monitoring method to identify and update details of the selfish node in that network. In Watchdog activity monitoring every nodes selfish or malicious behaviour is monitored and when a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non selfish node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this information to it; so, from that moment on, both nodes store information about these positive (or negative) detections. Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly. Using that way in our paper we identify selfish node whenever nodes in the network sending a chord key to neighbor nodes to tell their location in that network. If nodes come to identify any selfish node it will mark that node as a positive and update the details in node frame and send that details to neighbor nodes in the network group. Non selfish nodes will mark as a negative.

E. Route discovery

Usually MANET is a collection of mobile devices in wireless connectivity with minimum resources, restricted range of broadcast, and do not have fixed infrastructure. In MANET, route discovery is critical task because it is dynamically discovered process and security is one of major issue in MANET but we can achieve communication by forwarding data packet in appropriate routes and that routes are discovered dynamically and maintained between nodes in collaboration way. Once Source identifies routes from source node to destination node, it will forward data from that route.

F. Chord Algorithm

```
// New Chord ring creates
 m.create()
Predecessor = nil;
Successor = m;
//joining a node into Chord ring
m.join(m0)
predecessor = nil;
successor = m0.find successor(m);
//verifies m's immediate successor,
m.stabilize()
y=successor.predecessor;
if(y º (m;successor))
successor = y;
successpr.notify(a/b);
//mo thinks it might be our predecessor.
m.notify(m0)
if(predecessor is nil or m0 º (predecessor; m))
predecessor = m0;
//refreshes finger table entries
m.fix_fingers()
next = next+1;
if(next > n)next = 1;
finger[next] = find successor(m+2next-1);
//checks whether predecessor has failed.
m.check_predecessor()
if(predecessor has failed)
predecessor = nil;
```

IV. RESULT AND DISCUSSION

We evaluated the performance of chord in mobile adhoc network. Chord in MANET can be provides not only indirect, but also direct routing in conventional way. Our proposed system overcomes some critical problems of existing system. Our existing CoCoWa system, if identify any node as selfish then it send that details to other nodes, when it get contact of that nodes. In proposed system nodes find selfish node when it is moving message packet to next nodes and send that details to neighbor nodes in the network group. Chord nodes in MANET maintain the details of few nodes only so it reduces routing overhead. Chord in MANET addressing these problems also:

Load balance: MANET in Chord nodes use hash function in distributed way and spreading keys to all nodes in evenly. This provides load balance in network.

Decentralization: Decentralization is achieved by full distributed using chord technique: nodes need not give important to other nodes. It gives improved robustness and support to peer-to-peer nodes.

***Scalability*:** Cost of chord grows if number of nodes increases, so a large system is feasible. Parameter tuning is not required to achieve scaling.

A. Comparison of Overhead, Scalability Load balance with Chord Algorithm

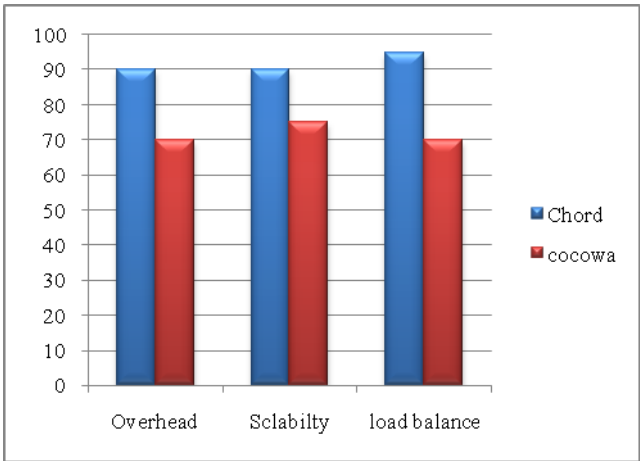

Fig. 2 Comparison of Overhead, Scalability Load balance with Chord Algorithm

The above Figure 2 illustrates that the chord algorithm overcomes some difficulties when compare to that existing scheme. It shows the advantage in Load balance and Decentralization using distributed way, and Overhead is achieved by the network construction technique. Cost of proposed system grows whenever the network capacity grows

B. Time of Selfish Nodes Detection

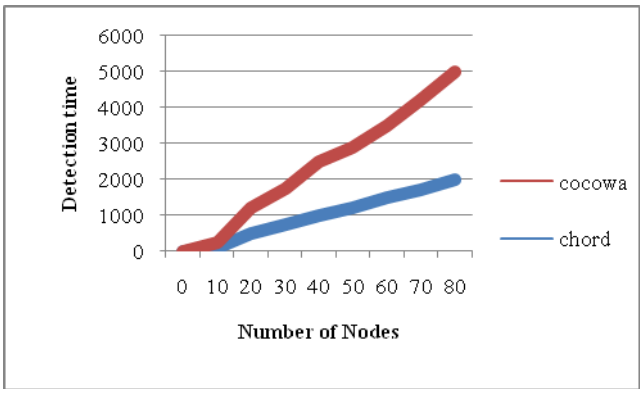

Fig. 3 Time of Selfish Nodes Detection

The above Figure 3 illustrates the time taken to detect selfish node in MANET. In existing it takes additional time to identify selfish node because it send the details to other node when a contact occur with other node. In Proposed it sends the information to neighbor nodes in the network once it identifies the selfish node

V.CONCLUSION

In this proposed system we use chord algorithm to identify selfish node. The Chord Algorithm does the following operation: gives key to nodes, maps that key to node and node send packet using that key. Chord in MANET is addressing some difficulties like provable correctness, performance and simplicity. In future work we concentrate to improve in following areas. Chord in MANET currently has no clear mechanism for partitioned rings; such type of rings could show consistent to stabilization procedure. Another approach to maintain memory in set of nodes in long-term memory, it is encountered in past; in partition forms, other partition nodes are likely to include the random sets.

REFERENCES

[1] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, (2009) “A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks”, (IJNSA), Vol 1, No 1.
[2] J.-P. Hubaux, T. Gross, J.-Y. L. Boudec, and M. Vetterli, (2000) “Toward self organized mobile adhoc networks – the termi nodes project,” IEEE Communications Magazine, vol. 39, no. 1, pp. 118–124.
[3] Sukla Banerjee, (2008), “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad- Hoc Networks”, in Proceedings of the World Congress on Engineering and Computer Science.
[4] A. S. Anand, M. Chawla, (2010), “Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET”, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1.
[5] Karger, D., Lehman, E., Leighton, F., Levine, M., Lewin, D., And Panigrahy, R. (1997) “Consistent Hashing And Random Trees: Distributed Caching Protocols For Relieving Hot Spots On The World Wide Web”. In Proceedings Of The 29th Annual Acm Symposium On Theory Of Computing ,Pp. 654–663.

[6] M. Anupama and B. Sathyanarayana, (2011) "Survey of Cluster Based Routing Protocols in Mobile Ad hoc Networks," International Journal of Computer Theory and Engineering, Vol. 3, Issue No. 6.
[7] T.V.P.Sundararajan, Dr.A.Shanmugam, (2010), "Modeling the Behavior of Selfish Forwarding Nodes to Stimulate Cooperation in MANET", International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2.
[8] Marko Jahnke, Jens Toelle, Alexander Finkenbrink, Alexander Wenzel, et.al; (2007), "Methodologies and Frameworks for Testing IDS in Adhoc Networks"; Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks; Chania, Crete Island, Greece, Pages: 113 – 122.
[9] Y.-C. Hu, A. Perrig, D. B. Johnson; (2006), "Wormhole Attacks in Wireless Networks"; IEEE Journal on Selected Areas of Communications, vol. 24, numb. 2, pp. 370-380.
[10] Yang, H. and Luo, H. and Ye, F. and Lu, S. and Zhang, U., (2004), "Security in Mobile Ad Hoc Networks: Challenges and Solutions", Wireless Communications, IEEE, vol. 11, num. 1, pp. 38-47.

AUTHOR PROFILE

Sathya bama B received the B.Tech degree in Information Technology from KCG College of technology (affiliated to Anna University) in 2014. She is currently doing M.Tech in the department of Information Technology in Sathyabama University, Chennai, Tamil Nadu, India.

Indira K received the M.Tech degree in Information Technology from College of Engineering, Anna University, in 2007. She is currently an Assistant Professor in the Department of Information Technology, Sathyabama University, Chennai, Tamil Nadu, India. Her research interests include Wireless Sensor Networks, Intrusion Detection System and Network Security.