DETECTION AND ISOLATION OF RELUCTANT NODES USING REPUTATION BASED SCHEME IN AN AD-HOC NETWORK

Rekha kaushik[1] and Jyoti Singhai[2]

[1]Department of Information Technology, MANIT, Bhopal, India.
rekhakaushik28@gmail.co.in
[2]Department of Electronics and Communication Engineering, MANIT, Bhopal, India.
j.singhai@gmail.co.in

ABSTRACT

In an ad hoc network, the transmission range of nodes is limited; hence nodes mutually cooperate with its neighbouring nodes in order to extend the overall communication. However, along with the cooperative nodes, there may be some reluctant nodes like selfish nodes and malicious nodes present in the network. Such nodes degrade the performance of the network. This paper, gives a survey of reputation based mechanism and credit based mechanism. These include different strategies by which non cooperative nodes are detected, isolated and/or prevented, their advantages and limitations. Also, a global reputation based scheme is proposed in this paper for the detection and isolation of selfish node. A cluster head is used which is responsible for reputation management of each node in the network. Detection of selfish nodes is accomplished which are created due to nodes conserving their energy using NS2. After their detection, performance analysis of network with selfish node and the network after isolation of selfish node is carried out.

KEYWORDS

Ad-hoc Network, DSR, Selfish node, reputation based mechanism.

1. INTRODUCTION

A Mobile Ad-hoc network (MANET) is a self configuring and infrastructure less network of mobile nodes. Each node acts as a router and is free to move independently in any direction. In an ad-hoc network, communication between two nodes beyond the transmission range relies on intermediate nodes to forward the packet. The communication between nodes takes place using routing protocol [1] which is of three types: Proactive, Reactive and Hybrid routing protocol.

Pro-active (table-driven) routing: This type of protocols, such as DSDV [1] maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantage of such algorithms is slow reaction on restructuring and failures.

Reactive (on-demand) routing: This type of protocols, such as DSR, AODV [1] finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are high latency time in route finding and network clogging due to excessive flooding.

Hybrid routing: This type of protocols combines the advantages of both proactive and reactive routing. The routing is initially established with some pro actively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice for

DOI : 10.5121/ijcnc.2011.3207

one or the other method requires predetermination for typical cases. The main disadvantage of such algorithms is that it takes long time when exploring new routes without a prior knowledge.

This paper uses DSR [1][2] which is a source routing protocol and this protocol can react to topological changes rapidly. Each node gathers information about the network topology by overhearing other nodes' transmissions. This is known as promiscuous mode of operation. DSR is a reactive routing protocol. There are two main operations in DSR; route discovery and route maintenance. DSR protocol tries to minimize the energy consumption by discovering routes to other nodes only when they are required. Each node maintains a route cache to remember routes that it has learnt about. All routing protocols including DSR assume that all nodes in a network are cooperative and forward others' messages.

The successful operation of MANET is totally dependent on the cooperation of participating nodes in communication. Lack of fixed infrastructure in ad hoc networks forces ad hoc hosts to rely on each other in order to maintain network stability and functionality. But sometimes nodes do not work as they were expected to and give rise to reluctant and/or malicious nodes.

In this paper, selfish nodes are detected using promiscuous overhearing of neighboring node when node drop packet due to nodes conserving their energy. Also, using reputation value and energy value of each node placed at cluster head, selfish node isolation is carried out. Simulation analysis of network is carried out using NS2. Along with the detection and isolation of selfish node using global reputation, this paper also gives a review on various types of reputation based and credit based mechanisms by which selfish and malicious nodes are detected, isolated and prevented.

The rest of the paper is organized as follows. Section 2 describes different types of non cooperative nodes. Section 3 is related work which includes reputation based and credit based mechanism. Section 4 shows the proposed reputation based scheme by which selfish nodes are detected and isolated. Section 5 shows the simulation setup then results are analyzed in next section. Section 6 describes conclusion and future work.

2. TYPES OF NON COOPERATIVE NODES

In an ad hoc network, the transmission range of mobile nodes is limited due to power constraint. Hence communication between two nodes beyond the transmission range relies on intermediate nodes to forward the packets. But sometimes these intermediate nodes do not work as expected, in order to conserve their limited resources such as energy, bandwidth etc. Such nodes are called non cooperative nodes or misbehaving nodes. They are of following types:

Malicious Nodes: If malicious nodes are present in a MANET, they may attempt to reduce network connectivity by pretending to be cooperative, but in effect drop any data they are meant to pass on. Several types of attacks are performed by malicious node like DOS attack, black hole attack, worm hole attack, rushing attack[3][4]. The attacks of malicious node on other nodes could be in the form of unnecessary route request control message, frequent generation of beacon packets or forwarding of stale information to nodes. These actions may result in defragmented networks, isolated nodes, and drastically reduced network performance.

Selfish Nodes: Selfish nodes [3][4] work in an ad hoc network to optimize their own gain, with neglect for the welfare of other nodes. Selfish nodes disturb the performance of ad hoc network to a great extent. When a node becomes selfish it does not cooperate in data transmission process and causes a serious affect on network performance. It simply does not forward packets of other nodes to conserve its own energy, bandwidth. Selfish nodes can be divided into two categories:

Category I: The nodes participate correctly in routing function but not forward data packets they receive to other nodes; so data packets may be dropped instead of being forwarded to their destination.

Category 2: The nodes do not participate correctly in routing function by not advertising available routes. For example: in DSR, selfish nodes may drop all RREQ they receive or not forward a RREP to some destination. Consequently, these selfish nodes will not participate in the requested routes.

3. RELATED WORK

Since enforcing node cooperation to facilitate transferring other nodes' packets is a major concern in an ad-hoc network. Most of the existing solutions are based on following mechanisms: reputation based, credit based and Reputation cum Credit based mechanism.

3.1. REPUTATION BASED MECHANISM

In Mobile Ad hoc network, Reputation systems are used to keep track of the quality of behaviour of other nodes. Basically reputation is an opinion formed on the basis of watching node behaviour by direct and/or indirect observation of the nodes, through route or path behaviour, number of retransmissions generated by the node , through acknowledgement message and by overhearing node's transmission by the neighbouring nodes [5][6][7][9][10][16][17].

One of the main goals/reasons for using reputation systems in a network of entities interacting with each other is to provide information to help assess whether an entity is trustworthy. This helps in detection of selfish and malicious nodes. Another goal is to encourage entities to behave in a trustworthy manner, i.e. to encourage good behaviour and to discourage untrustworthy entities from participating during communication.

A mechanism called Watchdog for the detection of non cooperating nodes, and Pathrater for rating of every used path are proposed in [5]. The watchdog mechanism is employed on each node individually to observe the message sent by neighbouring nodes. Comparison of the overheard messages with a list of messages that have to be forwarded reveals whether the observed node is forwarding the messages appropriately or not. This enables nodes to avoid non cooperative nodes in their routes. The limitation of this mechanism is that the misbehaving node gets isolated, so this becomes reward for misbehaving node and its sole intention of energy saving is accomplished. This algorithm can only detect the misbehaviour but unable to do anything to correct it.

CORE [6], a collaborative reputation mechanism , also has a *watchdog* component; however it is complemented by a reputation mechanism that differentiates between subjective reputation (observations), indirect reputation (positive reports by others), and functional reputation (task specific behaviour), which are weighted for a combined reputation value that is used to make decisions about cooperation or gradual isolation of a node. CORE permits only positive second-hand information, which makes it vulnerable to spurious positive ratings and misbehaved nodes increasing each other's reputation.

CONFIDANT [7] protocol uses reputation mechanism to identify and isolate selfish nodes. The protocol is based on selective altruism and utilitarianism, thus making misbehaviour unattractive. CONFIDANT consists of four important components - the Monitor, the Reputation System, the Path Manager, and the Trust Manager. They perform the vital functions of neighbourhood watching, node rating, path rating, and sending and receiving alarm messages, respectively. Each node continuously monitors the behaviour of its first-hop neighbours. If a suspicious event is detected, details of the event are passed to the Reputation System. Depending on how significant and how frequent the event is, the Reputation System modifies

the rating of the suspected node. Once the rating of a node becomes intolerable, control is passed to the Path Manager, which accordingly controls the route cache. Warning messages are propagated to other nodes in the form of an *Alarm* message sent out by the Trust Manager.

Self policing MANET [8], combines misbehaviour detection method with reputation system. Here each node can make its own decision on how to react to the behaviour of other nodes. Self policing provides a disincentive for cheating by excluding node from network. In this paper, author enhances CONFIDANT protocol and maintains two rating to make decision about the node: reputation rating and trust rating.

In [8], the mechanism relies on the principle that a node autonomously (without communicating with other neighbouring node) evaluates its neighbor based on the completion of request services. On successful delivery, reputation index increases else decreases. This can be done through TCP acknowledgement. It provides detection, prevention and punishment scheme to misbehaving nodes. In this paper, the author does not discuss about the value of reputation threshold chooses.

COSR [10] (Cooperative on Demand Secure Routing Protocol), is an extension of DSR protocol that uses reputation model to detect malicious and selfish behaviour of nodes and makes all nodes more cooperative. In COSR, Node reputation and Route reputation are measured using three parameters: *contribution of node* (how many route as well as data packet are forwarded between nodes), *capability of forwarding* packet of a certain node using energy and bandwidth threshold and *recommendation* which represent other's subjective recommendation. Advantage of COSR is that it is capable of avoiding hot points .It work well with blackhole, wormhole, rushing attack and selfish node but unable to handle DOS attack.

However, there are limitations of reputation based mechanism. First, as there is a possibility of collision, a packet will naturally drop even in the absence of a selfish node. This makes it difficult to ascertain whether the packet drop is due to natural reasons or selfish behaviour of node. Second, the selfish nodes isolated from the network using reputation based scheme cannot be used in data forwarding. This solution is trivial, but not efficient. Much approach does not punish nodes that do not cooperate since data is forwarded using a different path without complaint. Another limitation of reputation based system is that it often assumes that nodes that send reputation information about their peers are themselves trustworthy; and they are subject to collusion among nodes that misreport reputation information

3.2. CREDIT BASED MECHANISM

Credit based mechanisms reward nodes for forwarding by giving them credits. Without credit, a node cannot transmit self-generated data packets.

SPIRITE [11], an incentive based system in which selfish nodes are encouraged to cooperate. In this system, a node reports to the Credit Clearance Service, the messages that it has received/forwarded by uploading its receipts. Intermediate nodes earn credit when they forward message of others' node. In addition to the availability of central authority, sprite assumes source routing, and a public key infrastructure.

Chee–wah Tan and sanjay kumar bose propose an on demand routing protocol based on cost credit model [12] to enforce cooperation. By using the cost credit model, nodes can increases self transmission and also allows more data packet to be transmitted.

Limitations of this mechanism are, a virtual bank is required to manage credits and when a node has enough credits to send its own data, it can decide not to cooperate anymore and starts dropping packets. Also securing messages containing credits is also an essential requirement so that malicious node could not change credit value.

3.3. REPUTATION CUM CREDIT BASED SYSTEM

Secure and Objective Reputation–based Incentive (SORI) scheme [13] encourages packet forwarding and disciplines selfish behaviour in a non cooperative ad hoc network. Reputation of the node is used as an incentive for cooperate among nodes. Authors are able to design a punishment scheme to penalize selfish nodes.

ARM [14] selects low mobility nodes as reputation management nodes and is responsible for managing reputation values. ARM uses locality aware Distributed Hash Table for efficient reputation information collection and exchange. Advantage of using ARM is that ARM builds a hierarchical structure to efficiently manage the RVs of all nodes, and release the reputation management load from individual high mobility nodes. This enables low overhead and fast global reputation information accesses. Also ARM does not require currency circulated in the system.

From above literature survey, following issues will be considered to make comparison on different mechanism.

3.1.1. DETECTION OF NON-COOPERATIVE NODE

Both reputation based system and credit based system uses one of the following technique for the detection of non cooperative node. Promiscuous mode in [5] is used to overhear the communication of its neighboring node. In CORE, nodes do not only rely on promiscuous mode, but in addition they can judge the outcome of a request by rating end to end connection. In [7] monitor mechanism is used and neighbour watch mechanism is used by [10][13]. Retransmission of messages, route reply messages [9] and history or previous observations are also used by different authors to detect non cooperative nodes.

3.1.2. MANAGEMENT DEVICES

Some Reputation and Credit based mechanisms require extra management device or node for the management of reputation or credit. SPIRITE uses CCS for its credit management; ARM uses low mobility devices for reputation management. Other parameters to choose management nodes are high energy, locality and reputation table. This paper uses Cluster head as reputation manager.

3.1.3. ROBUSTNESS AGAINST NON-COOPERATIVE NODE

Systems like CONFIDANT, COSR are robust against non-cooperative node which system like CORE, SORI, ARM work well with selfish node.

3.1.4. ROBUSTNESS AGAINST COLLUSION

SPIRITE, CONFIDANT is collusion resistant system.

3.1.5. AUTHENTICATION MECHANISM

SPRITE uses cryptographic method and digital signature to prevent data from malicious node. The propagation of reputation is computationally-efficiently secured by a one-way-hash-chain-based authentication scheme. [14] Utilize hash chains to reduce number of digital signature operation.

3.1.6. GLOBAL / LOCAL REPUTATION

From above references it is carried out that reputation or credit value is kept either globally or locally. Each has advantage as well as disadvantage. In global Reputations each node maintains reputation values of every other node, so the size is O(N) while in Local Reputation each node maintains reputation values of the neighbor node that is located in one-hop. Global reputation needs an additional computational overhead to decide whether to accept or reject a warning message and to update the reputation table. Local reputations are less vulnerable to false

accusations than global reputations because it uses direct observation. Global reputation are less reliable as message traverse across the network so it could be delayed, modified, replayed or accidentally lost during transmission. Global reputation has better performance with respect to the mobility issue, because every node knows the behaviour of other node in the network so possibility to cheat is less.

4. PROPOSED SCHEME

This section represents the basic scheme of reputation based isolation of selfish node. The network architecture in figure 1 of proposed scheme consists of n number of mobile nodes and a clusterhead. In comparison to the previous mechanism, this scheme uses cluster head as a reputation manager. The advantage of using cluster head is that if it fails, a new cluster head take the responsibility.

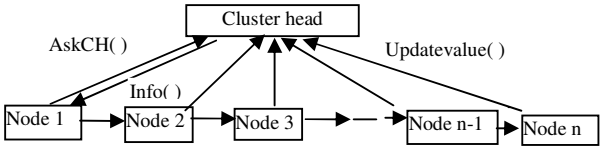

Figure 1: Architecture of proposed scheme

Assumptions: Some assumptions are considered for the proper operation of the scheme:

1. Energy threshold and reputation threshold are assumed as a fixed integer value.
2. It is assumed that cluster head fulfil all the criteria related to degree, location and association with other nodes in the network. It has sufficient energy and it does not misbehave.
3. Each node operates in a promiscuous mode, i.e., each node listens to every packet transmitted by its neighbours even if the packet is not intended for the node.
4. The parameters of each node in the network are almost same. For example, their transmission ranges and energy.
5. Nodes which want to send data already know the path to destination.

Proposed scheme works in three steps. Getting energy and reputation value of each node, Detection of selfish node and Isolation of selfish node from the network.

Let each node have fixed amount of initial energy NE and reputation value R. During the communication of packet, each node consumes a fixed amount of transmission energy (TE) and receiving energy (RE) consequently. At the instance where node energy drops below a pre defined threshold (E_THRESH), the node turns selfish, and drops all packets received from its neighboring nodes. Now if intermediate node forward packet correctly to its neighboring node, its reputation is increased by one else reputation value is decrease by one. If reputation of any node is less than a pre defined threshold (R_THRESH), node becomes selfish.

The value of each node's energy and reputation is kept at cluster head database table called ER list as shown in table 1.

Table 1: ER list consist of following information

Node ID	Node Energy	Reputation value

Where, Node ID is a unique id of each node.

The value of energy and reputation is updated through a small message called *updatevalue* containing values *(nid, energy, reputation).* Each time a node sends other's message to its

neighbouring node, it forwards *updatevalue()* message to the clusterhead for updating energy and reputation values in ER list.

At route discovery phase, each time a node wants to send its packet to other node, it first communicates using *AskCH*() with the cluster head , that knows about the node energy and reputation value of each intermediate nodes present in the path.

AskCH((sn_id, dn_id,int_nid (1,2,….)), r)

Where *AskCH*() is used to get value from clusterhead, *sn_id* is source node id , *dn_id* is destination node id , *int_nid* contain id of intermediate nodes . *r* is a random number key which is used between clusterhead and source node for encryption and decryption of message, so that no other node is capable of changing the message, thus preventing the message or data from different attacks from malicious node.

Cluster head sends a message

Info((sn_id, dn_id,int_nid (1.1,2.2,….)), r)

Where 1.1, 2.2 and so on contain value of energy and reputation of respective intermediate nodes with r.

If any node is found having low energy value and low reputation value, it is considered as selfish node. If selfish node is present in the path, isolation of such node is carried out by not appending the node in the path. Hence no packet is forwarded through that node and another path is chosen by the sender node.

Global reputation based approaches are considered less reliable since the transmission of packets in or across the network makes them susceptible to be delayed; modification, replay as well as accidental lose during their transmission. For this reason a security mechanism should be applied to the message.

5. SIMULATION SETUP

The performance study of selfish node has been done using NS-2 simulator [18]. NS-2 is a scalable simulation environment for wireless network systems.

The network which is used for simulation consists of 20 nodes placed randomly in 670x670 areas. Each node has a transmission range of 250m and moves at a speed of 10m/s. The total sending rate of all the senders of the multi-cast group, i.e. the traffic load is 1Mbps.

To assign the value of node energy, energy model is used. Every node has initial energy set to 1000 joules. Receiving and transmitting power of node is set as 1 watt.

For performance study of network, two different numbers of connections between nodes were chosen using different values in traffic generator with given simulation parameter as shown in Table 2.

Table 2: Simulation Parameters

Parameter	Value
Number of Nodes	20
Routing Protocol	DSR
Packet size	512 bytes

Traffic model of sources	Constant bit rate
Mobility model	Random way point
Max speed	15 m/s
Initial energy of node	1000 joules
Simulation time	25 sec

From above parameter two different cases are observed. In case I, two selfish nodes are detected and in case II, three selfish nodes are detected.

6. SIMULATION RESULT

Simulation analysis is carried out using NS2. In this scenario, the reluctant node will drop every incoming packet if that packet is neither from itself nor to itself. To overcome with reluctant node problem, proposed scheme is applied to improve the network performance.

To analysis the network performance, a comparison is made on the basis of node throughput and packet delivery ratio between a network with selfish node and that after isolation of the selfish node using the proposed scheme.

Node Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps).

Figure 2 and figure 3 shows throughput of the network with two and three selfish nodes present in the network respectively and the throughput of the network after isolation of network.

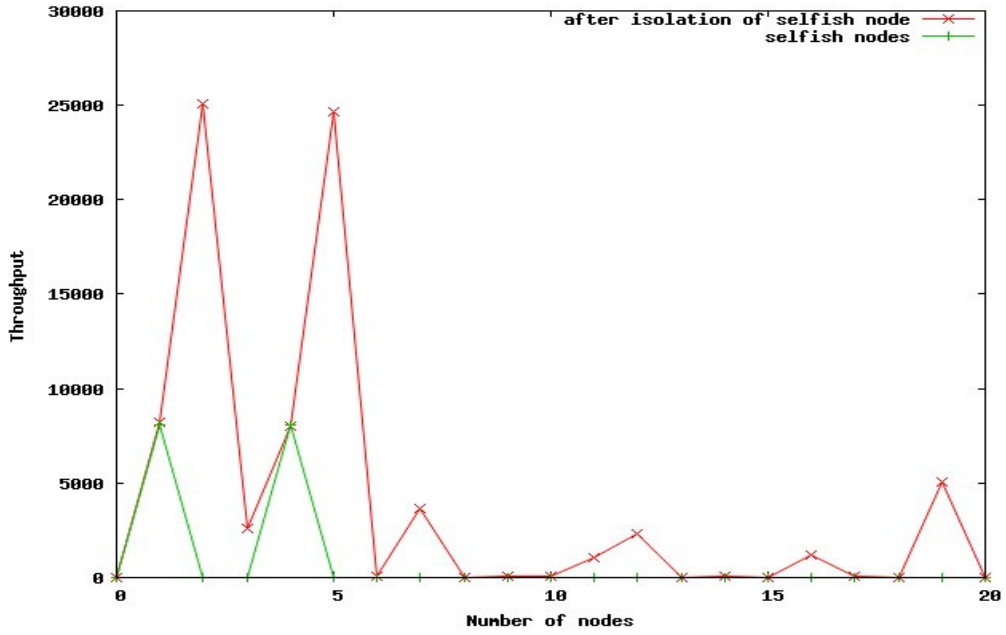

Figure 2: Throughput of ideal network and network with two selfish nodes

From figure it is clear that the throughput gets degraded in the presence of selfish nodes. As selfish nodes increases in the network the performance of the network degrades. When there are

2 selfish nodes present in the network throughput degrades by 80% and when there are 3 selfish nodes in the network throughput get degrade by 90%. Hence selfish nodes should be isolated from the network using the proposed scheme.

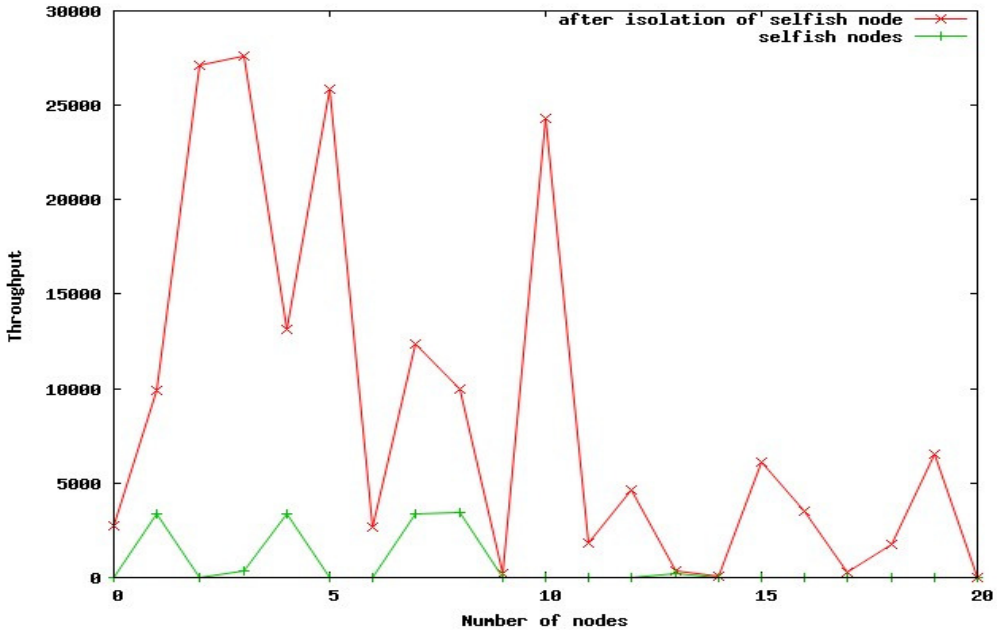

Figure 3: Throughput of ideal network and network with three selfish nodes.

Packet Delivery Ratio (PDR) is the ratio of total no. of packets sent to total no. of packets received.

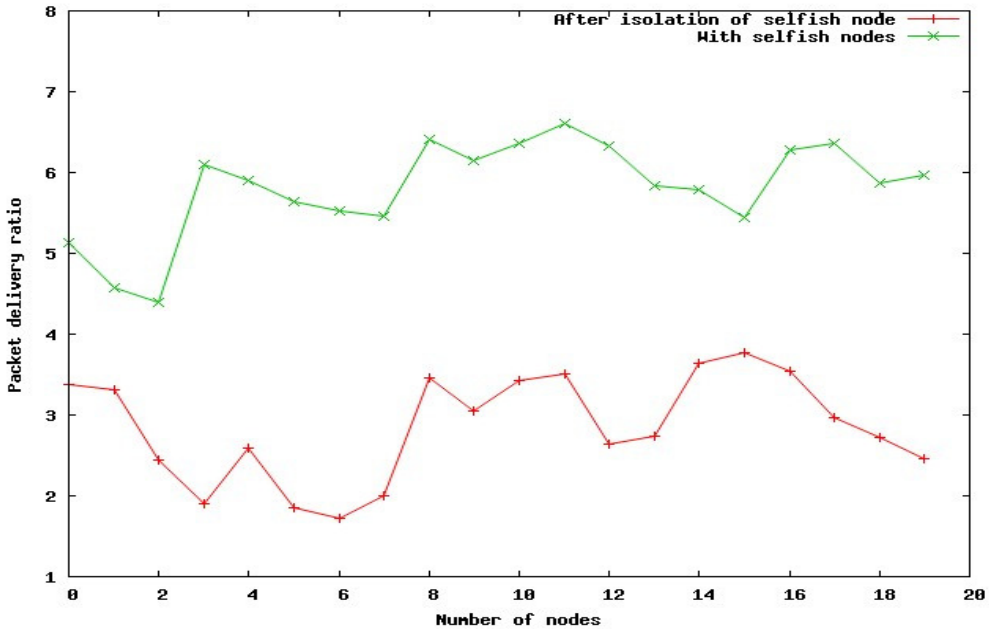

Figure 4: PDR of Network with 2 Selfish nodes and after isolation of Selfish nodes

Figure 4 and figure 5 shows the PDR when there when there are 2, 3 selfish nodes present in the network respectively and the PDF after isolation of selfish nodes.

It is analyzed from the data obtained by trace file that when there are 2 selfish nodes present in the network PDR increases by 50.8% and when there are 3 selfish nodes present in the network PDR increases by 65.2% as compared to the PDF after isolation of selfish node.

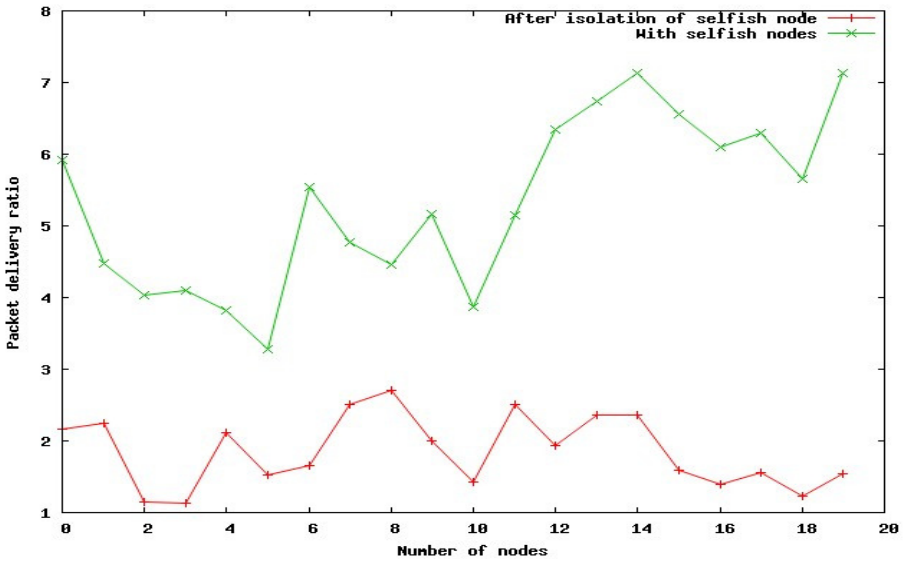

Figure 5: PDR of Network with 3 Selfish nodes and after isolation of Selfish nodes

7. CONCLUSION AND FUTURE WORK

This paper is the study of various reputations based and credit based mechanism which includes issues such as detection and isolation of non cooperative node, authentication mechanism, robustness, and management devices. Using these issues comparison of these mechanisms is done. These mechanisms help nodes to cooperate. With the insight gained from such an understanding, this paper proposes a new scheme based on node energy and reputation value to detect and isolate selfish node. Proposed scheme uses cluster head for keeping the value of energy and reputation of each node in a table. Security mechanism is also applied using cryptographic key so that message can be prevented from malicious node.

Proposed scheme is simulated using NS2.Performance evaluation of the scheme has been carried out which shows that the network throughput and packet delivery fraction increases after applying the proposed scheme.

For future work, the identity of the node can be hashed to further enhance the security. Also, malicious nodes may be taken into consideration.

REFERENCES

[1] E.Royer and C.K toh, (1999) ‘‘A Review of Current Routing Protocols for Ad hoc Networks”, IEEE Personal Communication Magazine, vol. 6, no 2, pp 46-55.

[2] D.Johnson , Y. Hu , D. Maltz, (2007) ‘‘The Dynamic Source Routing protocol (DSR) for Mobile Ad hoc network”, RFC 4728.

[3] Matthias Hollick, Jens Schmitt, Christian seipl, (2004) ‘‘On the Effect of Node Misbehaviour in Ad hoc Network” Proc. IEEE Conference on Communication, Vol 6, pp 3759– 3763.

[4] Nikos Komninos, Dimitris Vergados, Christos Douligeris, (2007) “Detecting unauthorized and compromised nodes in mobile ad hoc networks” Ad hoc Networks-Elsevier, Vol 5, Issue 3, pp-289-298.

[5] S.Marti, T. Giuli, K.Lai, M.Baker, (2000) "Mitigating routing Misbehaviour in Mobile Ad –hoc Networks", In Proc of the Sixth International conference on Mobile Computing and networking (MOBICOM), Boston.

[6] Pietro Michiardi and Refik Molva,(2002) "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks" Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia, .

[7] S. Buchegger and J-Y. Le Boudec, (2002) "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes, Fairness In Dynamic Ad-hoc Networks", Proc. of the IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC).

[8] Sonja Buchegger, Jean Yves Le Boundee, (2004) "Self – policing in Mobile Ad hoc Networks" In CRC Press, Chapter Handbook on Mobile Computing,.

[9] Tamer Refaei, Vivek Srivastava, LuizDaSilva, (2005) **"**A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks", Proc. IEEE Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05), pp 3-11.

[10] Fei Wang, Yijun Mo, Benxiong Huang, (2006) "COSR: Cooperative on Demand Secure Route Protocol in MANET", IEEE ISCIT, China, pp 890-893.

[11] S. Zhong, J. Chen, and Y. Yang, (2003) "Sprite: a simple, cheat-proof, creditbased system for mobile ad-hoc networks," IEEE INFOCOM, San Francisco, CA, USA, Vol 3, pp 1987-1997.

[12] Chee wah Tan, (2007) "Enforcing cooperation in an ad hoc Network using cost-credit based forwarding and Routing Approach", WCNC, IEEE, pp 2935-2939.

[13] Qi He, Dapeng Wu, Pradeep Khosla,(2004) "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks", WCNC / IEEE Communications Society, Vol. 2, pp 825-830.

[14] Haiying Shen and Ze Li, (2008) "ARM: An Account-based Hierarchical Reputation Management System for Wireless Ad Hoc Networks ,The 28th International Conference on Distributed Computing Systems Workshops, IEEE, pp 370-375.

[15] Hameed Janzadeh, Kaveh Fayazbakhsh, bahador bakshi, (2009) "A secure credit-based cooperation stimulating mechanism for MANETs using hash chains", Future Generation Computer Systems -Elsvier ,pp 926-934.

[16] Rekha kaushik, Jyoti Singhai (2010) "Simulation Analysis of Node Misbehaviour in an Ad hoc Network using NS2 " International journal of computer science and network security, Vol 8 , pp 179-182.

[17] A.V. Babu , Mukesh Kumar Singh (2010) "Node Isolation Probability of Wireless Adhoc Networks in Nagakami Fading Channel" International journal of computer networks and communications, Vol 2, pp 21-36

[18] NS2 network Simulator. http://www.isi.edu/nsnam/ns.

Authors

Rekha Kaushik holds a Master of Technology(2008) from BarKatullah University , Bhopal, M.P. India and Pursuing Ph.D from Maulana Azad National institute of Technology (MANIT), Bhopal , India. She is a member of CSI and ISTE. Her general research interests include wireless communication especially Ad-hoc network, network security.

Dr. Jyoti Singhai is Associate professor in Maulana Azad National Institute of Technology(MANIT), Bhopal, India. She holds Ph.D degree from MANIT, India. Her general research interests include wireless communication, image processing, and network security.