Detection of false alarm in handling of selfish nodes in MANET with congestion control

Ms. I.Shanthi[1] and Mrs. D. Sorna Shanthi[2]

**[1]Department of computer science and engineering,
Rajalakshmi engineering college,
Chennai, Tamilnadu, India-602105**

**[2]Department of computer science and engineering,
Rajalakshmi engineering college,
Chennai, Tamilnadu, India-602105**

Abstract

In a mobile ad hoc network, the mobile nodes will have the characteristics of mobility and constraints in resources. Since, the mobility is high, the nodes may move randomly and fastly, which lead to network partitioning. The resource constraints leads to a big problem as decrease in performance and the network partitioning leads to poor data accessibility. To improve the data accessibility, we have proposed several data replication techniques. Most of the users at different places assume that mobile nodes co-operate fully in terms of sharing their memory space. But In reality, some nodes may decide as not to co-operate with others or partially co-operate with other nodes. The behavior of these selfish nodes leads to decrease in over all data accessibility of the network. We have explored the impression of selfish nodes in a MANET from the perspective of replica allocation and developed selfish node detection algorithm that considers the partial selfish node and fully selfish node as selfish replica allocation. The replica will be allocated using specific SCF tree concept. An alarm will be raised based on the selfish behavior of overall nodes called overall selfishness alarm. But the alarm will also be initiated because of network disconnections too but it seems and treated as overall selfishness alarm, it will affect the overall performance of the network. The concept of the paper deals with detection of false alarm as differentiated from overall selfishness alarm and to inform the other nodes at route as exactly where the disconnections occur to select the next best alternative path and also to increase the performance with increased congestion control. Detection of attacker node in the network and should be informed to all others in the network.

Keywords: *mobile ad hoc network, selfish nodes, selfish replica allocation, crcn*

1. Introduction

MANET (Mobile ad hoc network) are dynamic networks populated by mobile stations. Stations in MANETs are usually laptops or mobile phones. These devices feature Bluetooth or Wi-Fi network interfaces and communicate in a decentralized manner. Mobile ad hoc networks are composed of a set of communicating devices able to spontaneously interconnect without any pre-existing infrastructure for it. Devices in specific range can communicate in a point-to-point fashion. More and more people are interested in mobile ad hoc networks.

Mobile networking is one of the most important technologies supporting pervasive computing. Mobility is a vital feature of MANET. Because of the high cost and lack of flexibility of such networks, experimentation is generally achievable through simulation.

During the last years, advances in both hardware and software techniques have resulted in mobile hosts and wireless networking common and diverse. Generally there are two different approaches for enabling wireless mobile units to communicate with each other:

1) Infrastructure - Based network: Wireless mobile networks usually been based on the cellular concept and depend on good infrastructure support, in which mobile devices communicate with access points like base stations connected to the stable network infrastructure.

2) Infrastructure less network: In infrastructure less approach there is no central administration for the entire network. The mobile wireless network is infrastructure less in manner commonly known as a mobile ad hoc network (MANET). A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing stationary network infrastructure.

MANETs have attracted a lot of attention due to the admiration of mobile devices and the advances in wireless communication technologies. Each node in a MANET must act as a router, and it should communicate with each other [1]. Network partitions can occur frequently because usually the nodes will move freely in MANET. But it cause

some data to be often inaccessible to some of the nodes. Hence, data accessibility is often a significant performance metric in a MANET.

Due to its great features of mobility and flexibility, MANET attracts different real world application areas whereas topology changes very quickly. MANET is more vulnerable than wired network due to node's mobility, dangers from compromised nodes inside the network, limited security, dynamic topology, scalability and lack of centralized management [2]. Because of these vulnerabilities criteria, MANET is more susceptible to malicious attacks.

Devices in MANET should be able to detect the presence of other devices around and it should perform the necessary set up to facilitate communication and sharing of data and service. Nodes that lie within each other's communication range can communicate directly are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each other's communication range, intermediate nodes acts as routers that relay packets generated by other nodes to their respective destination. The nodes at MANET is often energy-constrained such as battery, memory space. In our point of view we have taken the memory space as the constraint to find out the behavior of the node.

In MANET, breaking of communication link is very frequent, as nodes are free to move anywhere. The density of nodes and number of nodes are depends on the applications in which we are using MANET. The dynamic topology of MANET results in route changes and frequent network partitions and possibly packet losses. [3]

Data are usually replicated at nodes, other than the unique owners, to increase data accessibility to handle with frequent network partitions. A large amount of research has recently been proposed for replica allocation in a MANET. In general, replication can simultaneously improve data accessibility and reduce query response time if node have space to hold both all the replicas and the original data.

However, there is often a trade-off between data accessibility and query delay, because the most of the nodes in a MANET have only limited memory space [1]. For example, a node may hold a part of the frequently accessed data items locally to reduce its own query delay to get good performance. However, if there is only limited memory space and many of the nodes hold the same replica in their local memory space. Some data items would be replaced and missing by the replication process. Thus, the overall data accessibility would be decreased. A node should not hold the same replica that is also held by many other nodes. But however because of this replication process, there will be an increase in its own query delay [1].

1.1 MANET Features

MANET has the following features:

1).Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router. The ability and functions as a host, the mobile nodes can also perform switching functions as a router. So generally endpoints and switches are indistinguishable in MANET.

2).Distributed operation: Since there is no background network for the central control of the network operations, the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

3).Multi hop routing: Basic types of ad hoc routing algorithms can be single-hop and multi hop. Based on the diverse link layer attributes and routing protocols. When delivering data packets from a source to its destination out of the wireless broadcast range, the packets would be forwarded through one or more intermediate nodes. When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

4).Dynamic network topology: Since the nodes are movable in nature, the network topology may change quickly and randomly and the connectivity among the terminals may differ with time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network on the fly.

5).Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size.

1.2 MANET Applications

The set of applications for MANETs are ranging from large-scale to small scale environment, highly mobile and small and dynamic networks that are constrained by power sources. Some of the typical applications include:

1).Military battlefield: Military equipment now consistently contains some sort of computer equipment which will be useful for the security of the country. The mobile Ad hoc networking would allow the military to take advantage of common place network technology to maintain an information network in the military area. The communication deals between vehicles and soldiers.

2).Commercial sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood. Emergency rescue processes would takes place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed

3).Local level: MANET can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a place e.g. conference or classroom.

4).Personal Area Network (PAN): Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, cellular phone). Tedious wired cables are replaced with wireless connections.

5).Sensor network: This technology is a network composed of very large number of small sized sensors. These types of sensors can be used to detect any number of properties of an area. For Example, temp, pressure. The capabilities of each sensor are very limited and each must rely on others in order to forward data to a central server.

Automotive applications: Automotive networks are widely at research. Cars should enabled to talk to the road, to traffic lights and to each other. The network will provide the information about road conditions, congestions to the driver to optimize the traffic flow.

2. Selfish Node Behavior in MANET

Several nodes will be participated in the MANET for data forwarding and data packets transmission between source and destination. All the nodes of MANET will perform the routing function as mandatory. They must forward the traffic which other nodes sent to it. Among all the nodes some nodes will behave selfishly, these nodes are called selfish nodes.

MANET are Dynamic Topologies Bandwidth-constrained, variable capacity links Power-constrained operations Limited physical security.

A).Dynamic topologies Nodes are free to move arbitrarily; thus the topology of the network, may change randomly and rapidly at unpredictable times in network. Modification of transmission and reception parameters such as power may also impact the topology.

B).Bandwidth constrained: variable capacity links Wireless links will continue to have significantly lower capacity than their hard-wired counter parts. The relatively low to moderate link capacities will leads to the congestion rather than the exception.

C).Power-constrained operations: Some or all the nodes in a MANET rely on batteries for their energy. Thus, for these nodes, the most vital design problem may be that of power conservation.

Any node in MANET may act selfishly, which means, using its limited resource only for its own profit, since each node in a network has resource constraints, such as storage and battery limitations. A node would like to enjoy the profits provided by the resources of other nodes in the network, but however it should not make its own resource accessible to help others. Existing exploration on selfish behaviors in a MANET mainly focus on network concerns. For network problems at MANET may be as some selfish nodes may not transmit data to others to conserve their own battery constraints. Even though network disputes at MANET are important, replica allocation is also critical, ever since the vital goal of using a MANET is to provide data services to users [1].

We address the problem of selfishness in the context of replica allocation in a MANET. The problem because of replica allocation refers as if a selfish node may not share its own memory space to store replica for the benefit of other nodes. Selfish replica allocation refers to a node's

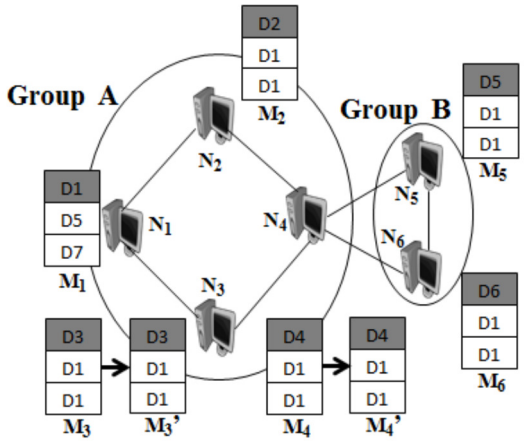


Fig 1.1 Example of selfish replica allocation

Non cooperative action, such that the node refuses to cooperate fully in sharing its memory space with other nodes. According to the figure, where nodes N1, N2... N6 maintain their memory space of nodes as M1, M2... M6, respectively, with the specified access frequency information in Table. As shown in Figure DCG seeks to minimize the duplication of data items in a group to achieve high data accessibility

Table 1.1 Access frequency table

Data	Nodes					
	N_1	N_2	N_3	N_4	N_5	N_6
D_1	0.65	0.25	0.17	0.22	0.31	0.24
D_2	0.44	0.62	0.41	0.40	0.42	0.46
D_3	0.35	0.44	0.50	0.25	0.45	0.37
D_4	0.31	0.15	0.10	0.60	0.09	0.10
D_5	0.51	0.41	0.43	0.38	0.71	0.20
D_6	0.08	0.07	0.05	0.15	0.20	0.62
D_7	0.38	0.32	0.37	0.33	0.40	0.32
D_8	0.22	0.33	0.21	0.23	0.24	0.17
D_9	0.18	0.16	0.19	0.17	0.24	0.21
D_{10}	0.09	0.08	0.06	0.11	0.12	0.09

2.1 Behavioral States of Selfish Nodes

We can define the behavioral states of nodes as three types in MANET from the viewpoint of certain constraints at memory space.

Type-1 node: The nodes are non-selfish nodes. These nodes can hold replicas allocated by other nodes within the limits of their memory space

Type-2 node: The nodes are fully-selfish nodes. These are the nodes which do not hold replicas allocated by other nodes, but it will allocate replicas to other nodes for their own accessibility.

Type-3 node: The nodes are partially- selfish nodes. These partially selfish nodes would use their own memory space partially for allocated replicas by other nodes. Their memory space may be separated logically into two parts: one is selfish area and another one is public area. These partially selfish nodes allocate replicas to other nodes for their accessibility.

The detection of the type-3 nodes is always complex, since they are not always selfish. In some situation, a type-3 node may be considered as non-selfish, since the node shares part of its memory space. But in our paper,, we have considered it as selfish node only, since these nodes also leads to the selfish replica allocation problem. Note that selfish and non-selfish nodes perform the same procedure when they receive a data access request, even though they behave differently in consuming their memory space.

2.2 Actions of Each Nodes at Specific Period

Each node detects the selfish nodes based on credit risk scores. Each node makes its own topology graph and builds its own SCF-tree by excluding selfish nodes. The topology graph may be of partial according to the particular node. Based on the concept of SCF-tree, each node in the network allocates replica in a fully distributed manner [1].
The CR score is updated during the query processing phase. With the degree of selfishness which we have measured, we intend a tree that represents relationships among nodes in a MANET, for replica allocation, termed the SCF-tree [1]. The SCF-tree models human friendship management in the real world.

When a node Ni makes an access request to a data item typically sending a query, the particular node will checks its own memory space first. If the requested item is present in its own local memory space then the request got successful. If it does not hold the original or replica, the request will be broadcasted to other nearby nodes which is connected to the node Ni. The request is also successful when Ni receives any reply from at least one node connected to Ni with one hop or multiple hops of nodes, which holds the original or replica of the targeted data item. Otherwise, the request fails.

Whenever a node Ni receives a data access request, it either 1) serves the request by sending its original or replica if it holds the target data item, or 2) forward the request to its neighbors if it does not hold the target data item.

3. Proposed Strategy

This chapter focuses on the mobile ad hoc network having selfish nodes and the way of replica allocation in the system helps to solve the data accessibility problem and about the simulation of system.

3.1 Detecting Selfish Nodes

In our strategy, each node calculates a CR score for all the nodes to which it is connected as its neighborhood. Each node at the network shall estimate the “degree of selfishness” for all of its connected nodes based on the CR score. We describe selfish features that may lead to the selfish replica allocation problem to determine both expected value and expected risk. Credit risk will

be calculated as the ratio of expected risk to the expected value.

Selfish features are classified into two groups: n query processing-specific and node-specific feature. In the query processing-specific feature, we develop the ratio of selfishness alarm which is the ratio of Node N1's data request being not served by the expected node Nk due to Nk's selfishness in its memory space. The query processing-specific feature can represent the expected risk of a node [1]. To effectively identify the expected node, Node N1 should know the (expected) status of other nodes' memory space. The SCF-tree-based replica allocation techniques support this assumption.

Node-specific features can be explained by considering the following case: A selfish node may share part of its own memory space, or a small number of data items, like partially selfish node. In this occasion, the size of shared memory space or the number of shared data items can be used to represent the degree of selfishness. The node-specific features can be used to represent the expected value of a node.

3.2 Building SCF-TREE

The main objective of our novel replica allocation techniques is to attain high data accessibility while reduce in traffic overhead. High Data accessibility is the prominent concern in all networks. If the replica allocation techniques allocate replica of the specified data item without any other node's concern, the traffic overhead will decrease.

Since the SCF-tree consists of only non-selfish nodes, we need to measure the degree of selfishness to apply in real-world friendship management to replica allocation in a MANET. We use the value of credit risk for building the tree. Before constructing or updating the SCF tree, node Ni eliminates selfish nodes from the base group INi.

The key strength of the SCF-tree-based replica allocation techniques is that it can minimize the communication cost, even though achieving high data accessibility. The high data accessibility is possible because each node detects selfishness and makes replica allocation at its own pleasure, without forming any group in the network.

Each node has a parameter d, the depth of SCF-tree. When N1 builds its own SCF-tree, N1 first appends the nodes that are connected to N1 by one hop to N1's child nodes. Then, N1 checks recursively the child nodes of the combined nodes, until the depth of the tree is equal to d. we assume that all nodes are non-selfish nodes for simplicity [1].

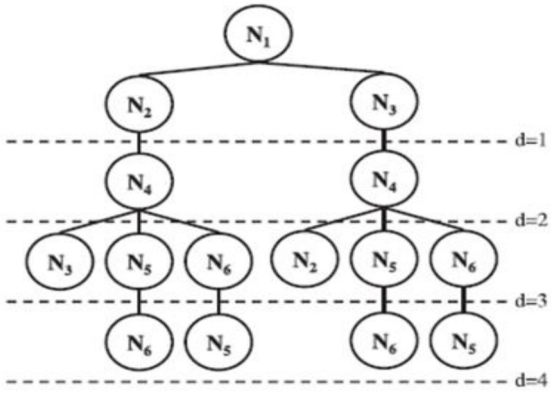


Fig 1.2 SCF tree for N1

As seen in Fig, the SCF-tree may have multiple routes for some nodes from the root node and that confer high stability. At every specific relocation period, each node in the network updates its own SCF-tree based on the network topology of that moment.

3.3 Replica Allocation

Each node allocates replica at its discretion based on Table and Fig mentioned above. When each node receives a request for replica allocation from Nk during a specific relocation period, the specific node solely determines whether to accept or reject the request. If the request is accepted by other node, the specific node will maintains its Mp based on the nCRki given by credit risk Table. If the highest nCRhi among the nodes which allocated replica to Ni, is greater than nCRki, Ni replaces replica allocated by node with replica requested by Nk.

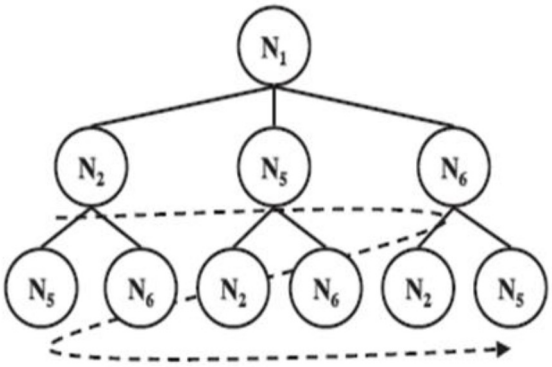
Table 1.2 Credit Risk table

N_i	N_k					
	N_1	N_2	N_3	N_4	N_5	N_6
N_1	·	0.30	0.85	0.80	0.45	0.22
N_2	0.40	·	0.80	0.90	0.30	0.50
N_3	0.25	0.35	·	0.75	0.65	0.75
N_4	0.45	0.44	0.51	·	0.23	0.37
N_5	0.30	0.60	0.85	0.40	·	0.21
N_6	0.40	0.50	0.90	0.52	0.30	·

Each node Ni executes this algorithm at every relocation period after building its own SCF-tree.

The node determines the priority for allocating replica items. The allocating replica priority is based on Breadth First Search (BFS) order of the SCF tree [1]. The dotted arrow in Fig.1.3 represents the priority for allocating replica. For example, in Fig.1.3, N1 selects N2 as the first target of the allocation in the tree. After allocating a replica to the last target node (i.e., N5 in Fig), the first node of the tree, N2 will be the next target in a round-robin manner. In our strategy, the target node could be the expected node

Fig 1.3 SCF based replica allocation



3.4 Detection of Attacker Nodes

A wired network under a single administrative domain allows for discovery, repair, response, and forensics of misbehaving nodes. A MANET is normally not under a single administrative area, making it challenging to perform any kind of centralized management or control. Hence here malicious nodes may enter and leave the immediate radio transmission range at random intervals, may collude with other malicious nodes to disrupt network activity and avoid detection [5].

After detecting some nodes as selfish node at the network, we would select an alternative path for the data packet transmission for a while. After a specific period of time every node will again start detecting the selfish nodes by measuring the degree of selfishness of all nodes in the network. But sometimes the attacker node, drops the packet without forwarding which will be very dangerous to our network also considered as selfish nodes. The attacker node in a network will be very prone to all sorts of attacks. Until the node misbehaves or alters any data in the network we cannot able to find it is an attacker. We will not take any actions against that node since us assuming that node as selfish node. In fact the node behaving as normal changed to selfish node only because of lack of the energy constraints and memory power. So a node cannot be selfish forever, whenever it get the constraints back it come back as normal node by indulging itself in normal data forwarding and sharing the space for other node's data.

If any attacker intrude inside a particular network it will leads to reduce in security of the data in the network. So we must identify the attacker node along with the selfish node. If a node acts as selfish for more than the predefined threshold value time then it will be considered as malicious or attacker. Each node at the network employs the mechanism that utilizes the neighborhood information to detect the misbehaving character of its neighbors.

At a specific interval the nodes will calculate the degree of selfishness of other nodes. After some 10 specific intervals, a particular node remains as selfish for all the time without any change then the node will be taken in consideration for the analysis of finding out whether it is malicious node or not. The neighborhood node of the particular node uses the detection mechanism to detect the misbehavior of specific node [5]. The mechanism is defined as whenever a particular node behaves abnormally the other node sent request will increase the malcount of the particular node. If the malcount of a particular node exceeds the predefined threshold value, then all the nodes of the network will be informed about the particular node.

After receiving that information all the other nodes at the network will be checks their local malcount for the broadcasted malicious node by analyzing the history and add the result to the initiator's response. All the nodes of the network will be constantly monitors the behavior of its neighbors and analyses it to detect if the neighbor has been compromised.

If neighborhood node detects the specific node as malicious, it propagates that information to throughout the network and waits for their responses. If two or more nodes has been reported about the particular node as same means then the malicious node will be isolated by other nodes. All the nodes which are using the malicious node as a route for their transmission will be in the process of discovering new routes. The detection of attacker node will be useful for avoiding future attacks.

3.5 False Alarm Detection

The false alarm will be differentiated from the overall selfishness alarm. If any alarm generated means we should verify the reason of the alarm. We should calculate the degree of selfishness again and to confirm the behavior of selfish nodes at the network. If the number of selfish nodes exceeds the threshold value means it will get confirm as overall selfishness alarm else the alarm has been raised because of the network disconnections. We should

diagnose the network disconnections by use of false detection algorithm. If it became true we should neglect the alarm with of less concern. The detection of this false alarm leads to better performance in the overall network.

The system using DSR protocol for the data transmission. The key distinguishing feature of DSR is the use of source routing. In the protocol, the sender knows the wide-ranging hop - by-hop route to the endpoint and these routes are stored in a route cache. The source route is carried by data packet in the packet header. When any node in the network tries to send a data packet to a destination for which it does not already know the route, then it follows the process of route discovery to discover the new path with dynamism.

Generally thuds protocol is composed of two processes that work together to allow the discovery and maintenance of source routes in the ad hoc network:

Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to Destination. Usually the route discovery mechanism is used only when Source node attempts to send a packet to Destination and does not already know a route to Destination.

Route Maintenance is the mechanism by which Source node is trying to explore, while using a source route to the Destination, if the network topology has changed such that it can no longer use its route to the Destination, because a link along the route no longer works.

There may be any network disconnections can happen over the route. When Route Maintenance specifies and informs that the source route is broken or destroyed, the Source node which needs to send data can attempt to use any alternate route it chances to know the Destination node, or can invoke Route Discovery again to find a new route. Route Discovery and Route Maintenance each operate entirely on request. In particular, DSR does not require periodic packets of any kind at any level within the network.

Cognitive radio network is a new emerging exploration area. Cognitive radio network enhances the existing software-defined radio, whose physical layer behavior is mostly defined in software. Usually Cognitive radio has the following characteristics. Initially, it is aware of its environment and its capabilities. Next, it is able to independently alter its physical layer behavior based on its previous experience and its current atmosphere. Lastly, it is capable of carrying out the complex adaptation strategies according to the cognitive cycle shown in.With these capabilities, when spectrum environment changes around cognitive user, it is proficient of recognizing these changes and independently changing its physical layer settings.

Though, there is no existing simulator that is suitable for the demand of cognitive radio simulations. Several researchers implemented their algorithms for cognitive radios on existing network simulator such as NS-2, OPNET, and QUALNET. There is a demand to extend existing simulators to support cognitive radio simulators.NS2 is the most popular simulator to implement the concepts related to wireless networks We make use of existing NS-2 to lengthen it to support cognitive radio network simulation.

In a group of nodes Source will discover a route for the destination to reach the data packets and keep sending the data through that route. CRCN always checking the transmission range around those networks. It will find the network disconnections when the first selected paths node got move from out of transmission range. Whenever the mobility range of any node at the specific route gets higher and it leads to network disconnections. The CRCN will detect the disconnections by recognizing when the transmission range of the nodes exceeds from the specific limit of range. After disconnections occur, false alarm will be raised. All the nodes will be intimated as this alarm is a false alarm and to ignore this alarm. But the nodes at the specific route alone should be intimated as where the disconnection occurred and should search an alternative path to reach the destination.

Already a lot of disconnections and link failure will be in the network. So we have to send the false alarm through the path which having no disconnections. But anyway we will have some half incomplete messages in the way of routing nodes. After disconnections we have to inform those node to delete those incomplete messages to avoid the waste of memory space.

4. Congestion Control

In mobile ad hoc network (MANET), congestion is one of the most important restrictions that deteriorate the performance of the whole network. It is essential to adjust the data rate used by each sender in order not to overload the network, where multiple senders compete for link bandwidth. The Packets at the network may be dropped when they reach the router and cannot be forwarded. Many packets are dropped while excessive amount of packets arrive at a network bottleneck. The packets dropped would've traveled long way and in

addition the lost packets often trigger retransmissions. This intimates that even more packets are sent into the network. And so, network throughput is still more worsened by the phenomenon called network congestion. There is a high probability of congestion collapse where almost no data is delivered successfully if no appropriate congestion control is performed. [6]
Using CRCN in MANET we can reduce the congestion rate at the network. The cognitive radio senses the data flow of the network and provides the increased data rate to the network. The use of cognitive radio cognitive networks provides increase in the packet delivery ratio of the network.
The simulation shows that the performance has been increased in packet delivery ratio and reduced communication cost with the use of cognitive radio cognitive network.

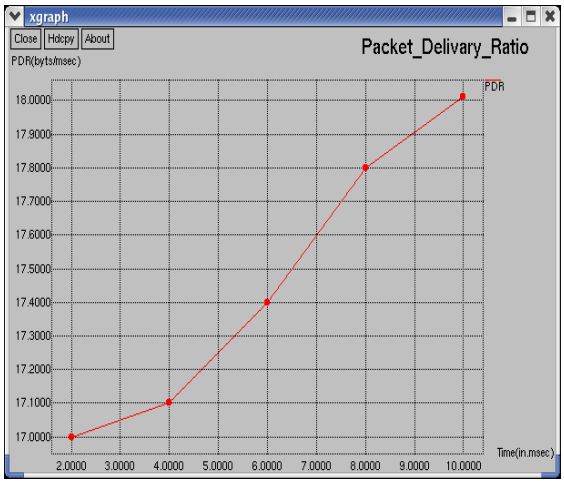


Fig 1.4 Packet Delivery Ratio

In the system we have implemented a selfish node detection method and novel replica allocation techniques to handle the selfish replica allocation. The proposed schemes are inspired by the real-world observations in economics in terms of credit risk and in human friendship management in terms of choosing one's friends completely at one's own decision. We have applied the concept of credit risk from economics to detect selfish nodes. Each and Every node in a specific network calculates credit risk information on other connected nodes individually to measure the degree of selfishness.

The system performance are extensively significant in the detection of attacker and to provide congestion control at MANET. Extensive simulation shows that the proposed strategies outperform the cooperative replica allocation techniques in terms of data accessibility, communication cost, and query delay. The False alarm at selfishness will decrease the data flow of the network. By using our technique we will pass the information as it is not by selfishness. So no significant change will occur except choosing for alternative routes. As a part future, we plan to consider all the replication strategies and network disconnections suited for various consistency level and with increase in security against various attacks. Our next goal will be to conduct an analytical study of the impact of node mobility on network performance with misbehaving nodes. We plan then to design and evaluate a collaborative security scheme that solves the selfishness problem, analyzing the effects of such mechanism on network throughput and communication delay.

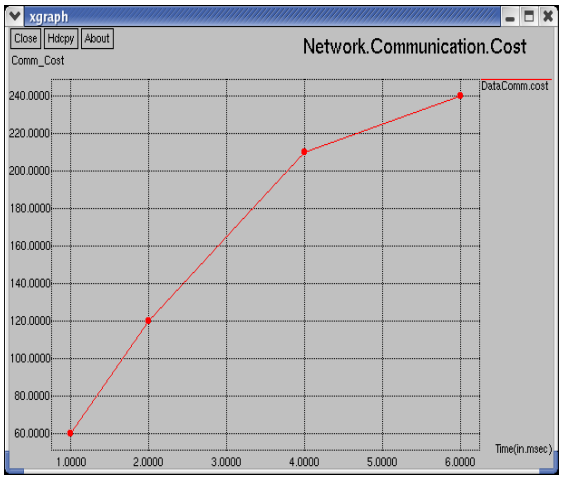


Fig 1.5 Network Communication Cost

5 Bibliography

[1]Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu"Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network" IEEE Transactions on mobile computing, vol. 11, no. 2, February 2012.
[2]Priyanka goyal,Rahul rishi, vinti parmar "MANET: Vulnerabilities, Challenges, Attacks, Application" IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011
[3]Mohit Kumar and Rashmi Mishra "An Overview of MANET: History,Challenges and Applications" Indian Journal of Computer Science and Engineering (IJCSE).
[4]Sonali Bhargava and Dharma P. Agrawal " Security Enhancements in AODV protocol forWireless Ad Hoc Networks"2004
[5]C. Lochert, B. Scheuermann, M. Mauve, "A Survey on Congestion Control for Mobile Ad-Hoc Networks", Wiley Wireless Communications and Mobile Computing 7 (5), pp. 655-676, June 2007
[6]T. Hara, "Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility," Proc. IEEE INFOCOM, pp. 1568- 1576, 2001.
[7]L. Anderegg and S. Eidenbenz, "Ad Hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad Hoc Networks with Selfish Agents," Proc. ACM MobiCom, pp. 245-259, 2003.

[8]K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," Proc. IEEE Wireless Comm. and Networking, pp. 2137-2142, 2005.
[9]H. Li and M. Singhal, "Trust Management in DistributedSystems," Computer, vol. 40, no. 2, pp. 45-53, Feb. 2007.12. M. Li, W.-C. Lee, and A. Sivasubramaniam, "Efficient Peer-to-PeerInformation Sharing over Mobile Ad Hoc Networks," Proc. WorldWide Web (WWW) Workshop Emerging Applications for Wireless andMobile Access, pp. 2-6, 2004
[10]S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," Proc. ACM MobiCom,pp. 255-265, 2000.
[11]K. Paul and D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR Based Ad-Hoc Networks," Proc. IEEE Global Telecomm. Conf., pp. 178-182, 2002.
[12]J. Zhai, Q. Li, and X. Li, "Data Caching in Selfish Manets," Proc.Int'l Conf. Computer Network and Mobile Computing, pp. 208-217,2005.
[13]T. Hara and S.K. Madria, "Consistency Management Strategies for Data Replication in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 8, no. 7, pp. 950-967, July 2009.
[14]S.-Y. Wu and Y.-T. Chang, "A User-Centered Approach to Active Replica Management in Mobile Environments," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1606-1619, Nov. 2006.
[15]N. Laoutaris, G. Smaragdakis, A. Bestavros, I. Matta, and I. Stavrakakis, "Distributed Selfish Caching," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 10, pp. 1361-1376, Oct. 2007.
[16]P. Michiardi and R. Molva, "Simulation-Based Analysis of Security Exposures in Mobile Ad Hoc Networks," Proc. European Wireless Conf., pp. 1-6, 2002.

I.Shanthi acquired her B.Tech degree in Information Technology under Anna University at Arunai engineering college in 2011 and currently pursuing M.E Degree in computer science and engineering under Anna University Chennai at Rajalakshmi engineering college, Chennai. Her area of interest includes networks and image processing and analysis.

Mrs.D.Sorna Shanthi has a teaching experience spanning over 9 years in the field of computer science and engineering. She acquired her B.E degree in Kamaraj engineering college at virudhunagar and completed her M.Tech degree in Sathyabama University in specialization of computer science. She is presently working at Rajalakshmi engineering college as Assistant Professor. She was formerly in valliamai engineering college. Her area of interest includes networks.