REVIVAL OF SELFISH NODES IN CLUSTERED MANET

[1]Santhosh Kumari D, [2]Thirunadana Sikamani K
[1]Research Scholar, Department of Electronics & Communication Engineering,
St. Peter's University, Chennai, India
[2]Professor and Head, Department of Computer Science and Engineering,
[2]St.Peter's College of Engineering & Technology, Chennai, India.

ABSTRACT

Mobile Ad hoc networks (MANETs) are proliferating into every application area of wireless technology due to the portability of the communication. In this paper we propose Revival of Selfish nodes (RSC) in clustered MANET. In this paper, selfish nodes present in the network are exploited for and encouraged to co-operate with the other nodes, thereby improving the network performance. RSC significantly reduces energy consumption as well as improved network lifetime. Simulation results obtained using Network Simulator 2(NS-2) indicate that the lifetime and quality of service is improved by RSC in MANETs. A case of homogeneous networks moving randomly in a fixed topology area is used for simulation analysis.

KEYWORDS: *MANET, Selfish behavior, Energy.*

I. INTRODUCTION

MANET is the most relevant area of research mainly because of the various challenges that it poses to the existing protocols and architectures. MANETs are wireless infrastructure less, autonomous networks and self organizing networks. Owing to their inherit characteristics such as no centralized control and limited energy resources, MANETs are susceptible to various vigorous and flaccid attacks. Additionally, most of the routing protocols proposed for MANET operate on the hypothesis that all the nodes must cooperate in routing operations such as packet forwarding, route discovery and route maintenance process. MANET nodes are necessary to cooperate with other nodes in forwarding packets and delivery services. In MANETs, nodes are varied such as mobile phones, laptops and belong to different persons gathered in the same environmental area for some reasons. These nodes can communicate each other that an individual node unselfishly spends its inadequate resources for helping other nodes. Conversely, this cooperation leads towards in which each node consumes its insufficient resources, such as battery power. The limited energy resource can prompt nodes to avoid take part in network services for other nodes, whilst still enjoying the network service. The nodes display such activities are considered as selfish.

Talreja and Jethani [2] proposed selfish node use the network for their individual communication but just reject to cooperate in forwarding packets for other nodes to facilitate save battery life. A selfish node would thus use the benefits provided by the resources of other nodes, but will not make available its own resources to help others. The selfish node does not cooperate jointly the normal node in the main reason for saving battery power. As a result we propose a Revival of Selfish node in clustered MANET.

The rest of this paper is organized as follows. In section II, related works are described. In section III, the proposed RSC is detailed, which is followed by the simulation and analysis in section IV. In section V, conclusion and finally the future works are discussed.

II. RELATED WORK

Djenouri and Badache [4] proposed security mechanism is necessary which keeps record of node's public and private key. While a node forwards a packet to the next node in the route it generates a

random number and encrypts it with the public key of node. Once the two hops lost node received this packet it decrypts and send the same random number as an acknowledgement. Acknowledgement is authenticated by the node's public key and some encryption method. But the node does not received acknowledgment by two hops left node and it indict the one hop away node as selfish. The 2 ACK receivers, monitors the link periodically by maintaining the information about the no of data packets sent and the no of data packets does not acknowledged within the period. Samreen and Narasimha [1] explained 2ACK technique detects the misbehaving link but cannot decide the connected node in which nodes are misbehaving thus, PFC monitoring as to detect the misbehaving nodes once the misbehaving link is detected. Hernandez-Orallo [3] introduced Watchdogs to detect selfish nodes in computer networks. A watchdog is the collaborative approach. The analytical model is evaluating the detection time and cost of this collaborative approach. Watchdog can significantly reduce the overhead and decrease overall detection time. Also improve the accuracy. Hernandez-Orallo et al [7] proposed CoCoWa (Collaborative Contact-based Watchdog) method is a collaborative based on the diffusion of local selfish nodes alertness thus that information about selfish nodes is rapidly propagated. This approach reduces the time and increases the accuracy while detecting selfish nodes.

Hussain et al [6] proposed selfish node detection which contains two major considerations. First, it focuses on the factors that induce appropriate nodes to act self-interestedly. Second, it proposed a slightly light-weight mechanism in terms of low energy consumption. This method consists of three main modules such as monitoring, data collection and detection. Tarannum and Pandey [11] explained detecting and removing the misbehaving node as well as improved the performance of the system by reentering the false detected node in network. This scheme consists of Data Gathering and Processing, Decision Making, and Response Operation. Gathering and Processing Module of the system collect data in two ways; first it locally runs a monitoring process to get the behavior information of neighbor nodes and secondly it exchanges this information with other nodes monitored information. This module is used as a data processing unit.

Manchikalapudi et al [8] proposed that every node in the network monitors the activities of its neighbors and if any irregular action is detected it invokes an algorithm to conclude whether the assumed node is definitely selfish. This mechanism builds trust in the network by communications between some defense components. The components at each node are supervisor, aggregator, trust calculator and disseminator. Supervisor module monitors neighbors by passively listen to their communication. This module uses Passive Acknowledgement (PACK) mechanism that checks whether the neighbors really forward the packets or drops them. Aggregator module collects all the details of the communication that can be used to estimate the number of packets dropped. Trust calculator is determined by the percentage of packet dropped. The percentage is treated as fuzzy input variable and the output of the algorithm is trust level of a node.

Muthumalathi and Raseen [9] introduced that every node can approximate the degree of selfishness intended for all of its connected nodes based on the Credit Risk (CR) score. CR is calculated based on the average of credit risk and expected value. Selfish features are two categories such as Node specific and Query processing specific. Node-specific features represent the size of shared memory space and the number of shared data items can be used to represent the degree of selfishness. The query processing-specific feature can represent the expected risk of a node. Every node has its own threshold value. The measured CR when exceeds the threshold node will be detected as a selfish node.

Kargl et al [5] explained an algorithm which can be classified into two main categories; the first is detection and exclusion whereas detection is to detect the selfish nodes and isolate them from network and the second one is motivational that is perceive selfish nodes and induce them to cooperate in network. MIMO (Multi-Input and Multi-Output) was proposed by Rachedi and Badis [10]. It allows the monitor node to avoid the collision during the monitoring process by adjusting the antennas weights in order to invalidate the signal coming from other nodes than the monitored one.

Sundararajan and Shanmugam [12] proposed energy saving is the only reason assumed for a node is selfish. Hence the node is acting selfishness based on residual energy. While the node has highest energy, the node is capable to supply more cooperation as well as more packet delivery ratio. Sujit and Pinaki [13] proposed the selfish node detection and punishment is very important issue and makes the nodes cooperative in nature in case of transferring data. Replica allocation technique is very efficient for co-operating the selfish node to other nodes. It is used to make the selfish node cooperative to other nodes. The network is disrupted such that the nodes are not dependable for

forwarding packets. This technique is applicable for all nodes that are having data items of other nodes. When the data transmits from one node to other nodes, allocation of memory space of every node is responsible for communication. If one node is selfish in the network the memory space of selfish node doesn't take the data items of other neighbor. In favor of forwarding packets through the selfish nodes copy the data items of neighbor nodes into the memory space of selfish node explicitly and make the selfish node cooperative to other nodes.

Reputation based and Credit based technique for detection of selfish node in MANETs was proposed by Dipali and Supriya [14]. 2ACK system uses the Reputation based approach to identify and diminish the consequence of misbehaving nodes in MANET. As well as arduous the selfish nodes and cheering the cooperating nodes there is second option for the nodes are dropped a packet reluctantly. This approach made the node to be a selfish node and punished. Thus cooperation coefficient is increased then it changes its behavior.

III. PROPOSED METHOD

A lot of protocols are suggested to enforce corporation and to find misbehaving nodes. In network, two or three nodes can be easily identified and detected. Sometimes most of nodes act as selfish nodes and all nodes are detected and removed. Therefore, the remaining nodes will not perform well.

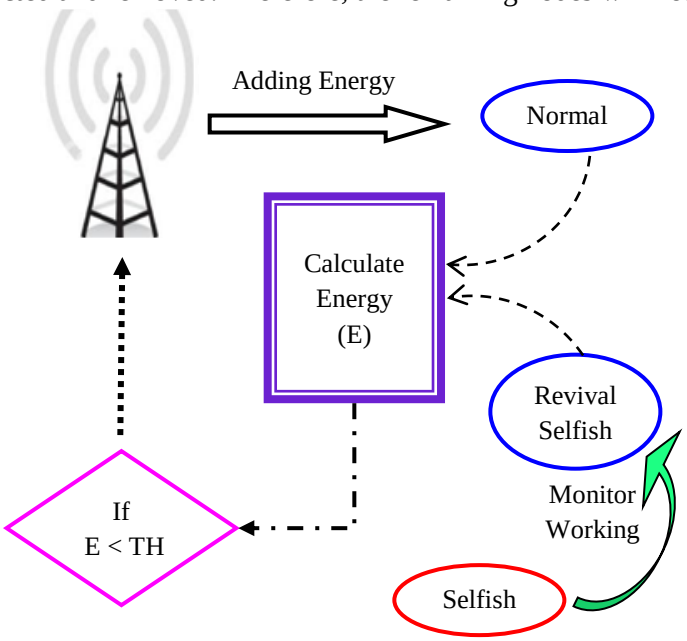

Fig 1: Revival of Selfish node Architecture

The existing scheme aims to Detect and Mitigate Selfish node (DMS) in MANETs. In this scheme, the selfish nodes do not co-operate other nodes. To overcome this problem, we propose Revival of Selfish nodes in clustered MANET. In this scheme, the selfish node cooperates with normal node. The node is acting s selfish because of saving the energy. If a selfish node is convinced about its necessity; selfish nodes automatically behave as the normal nodes.

In this scheme, the base station sends a pilot message to the all nodes. Normal nodes will respond to the message. The selfish node does not respond. The normal nodes are combined together to form a cluster. Then base station is decided by the cluster head.

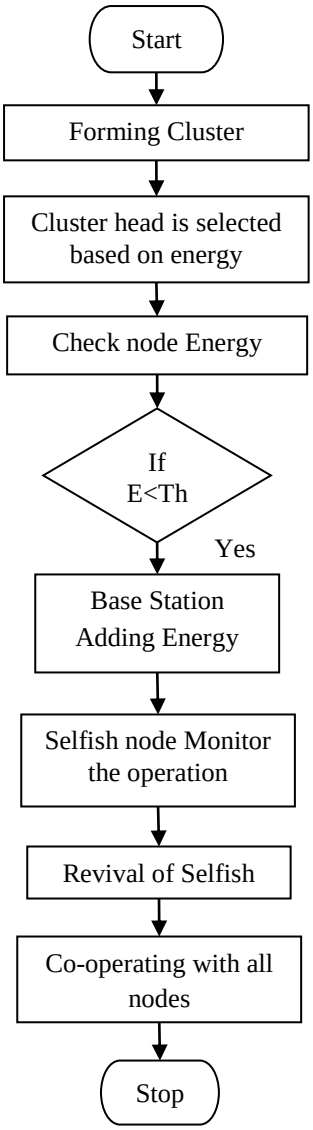

Fig: 2 Flowchart of proposed system

The cluster head is selected based on energy. The node with highest energy is selected. The cluster members send information to the cluster head. The normal nodes send data from source to destination. The nodes are cooperating to all nodes; the residual energy is reduced automatically. If the residual energy is less than threshold, then the base station provides the energy. Therefore, the energy in the node doesn't get dried. So the normal nodes are not dead. Also, this process is monitored by the selfish node and the selfish nodes are converting to the good behavior node. Then the selfish nodes are cooperating to the all nodes.

Fig 2 explains the process of Revival of selfish nodes. Initially the cluster is formed based on the distance and the cluster head is selected based on the node with high energy. The Data transmission nodes check the energy. If the energy is less than the threshold, the base station will add the energy. This process is monitored by selfish node and revival of selfishness then cooperates to all nodes in the networks.

IV. SIMULATION AND ANALYSIS

The simulation analysis is performed using the network simulator. To ensure that the proposed scheme is more efficient than the existing scheme, we have performed simulations to assess some of the vital parameters. The parameters in the table 1 below show how the simulation experiments have been performed.

Table 1: Simulation Parameters

Parameter	Value
Simulation Area	800x800
Simulation Time	50ms
Channel Type	Wireless Phy
Radio Model	Two Ray Ground Model
MAC Type	IEEE 802.11
Antenna Type	Omni Antenna
Mobility Model	Random Way Point
Number of Nodes	38

The RSC routing performance is obtained by comparing it against the DMS protocols using the parameters packet delivery rate, throughput, loss and delay and residual energy.

4.1. Packet Delivery Rate

Packet delivery rate is the ratio of number of packets delivered to all receivers to the number of data packets sent by the source node. It is measured by the equation 1 below.

$$PDR = \frac{Packets\,\text{Received}\,Rate}{Packets\,\text{Sent}\,Rate} \quad (1)$$

The figure 3 shows that the proposed scheme RSC has better packet delivery rate when compared to existing scheme DMS.

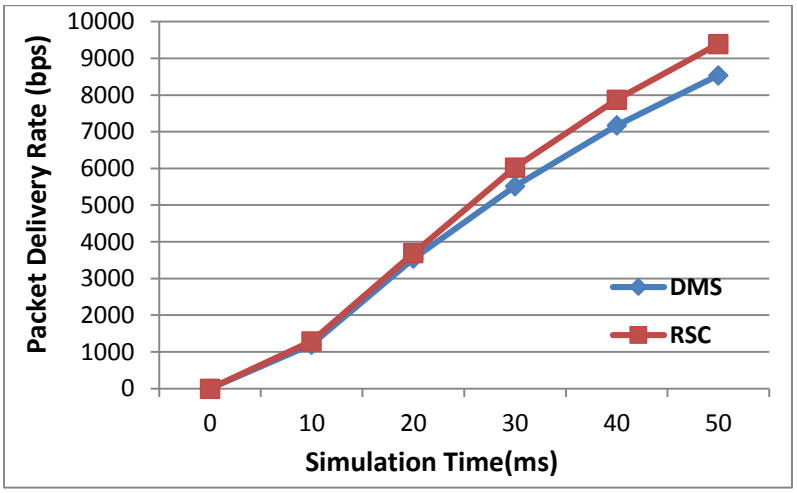

Figure 3: Packet Delivery Rate

4.2 Packets Lost Rate

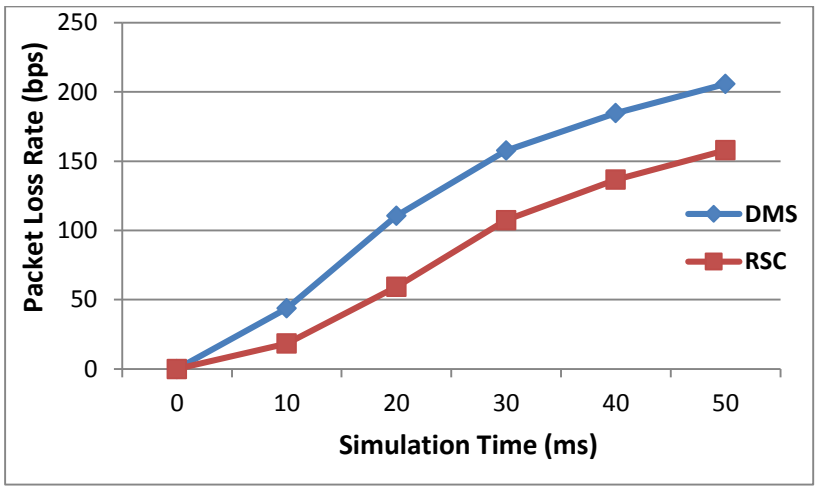

Figure 4: Packet Lost Rate

Packet Loss Rate is the number of packets lost over time in the network. Figure 4 shows that the DMS has heavy packet loss while compare to the proposed scheme.

4.3 Throughput

Throughput is the amount of data received by all the destinations in the network. The throughput is one of the main efficiency parameters used to assess the network.

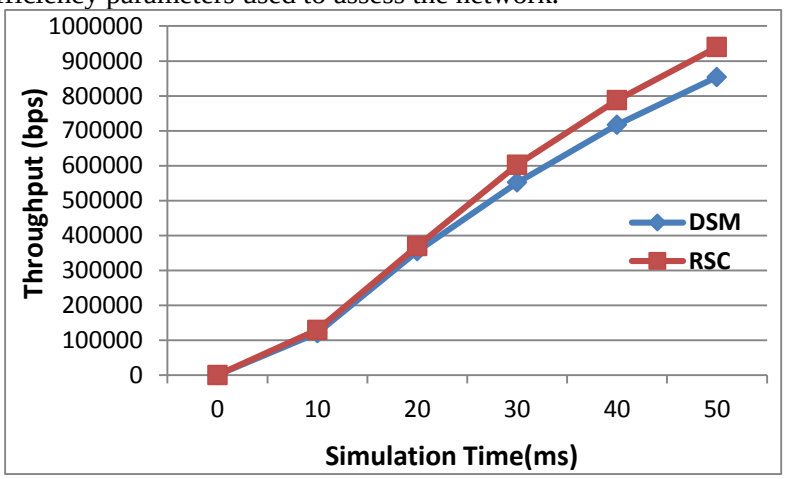

Figure 5: Throughput

Fig 5 indicates that RSC protocols perform better than DSM in the network.

4.4 Average Delay

The average delay occurring in the network is plotted in the figure 6 below. This is average time delay occurred in all the nodes during the operation of the protocol in the network. The time delay is greater for DSM compared to the RSC protocols. n represent number of nodes.

$$Avg\ Delay = \frac{\sum_0^n Sent\ Time - \text{Re}ceived\ Time}{n} \quad (2)$$

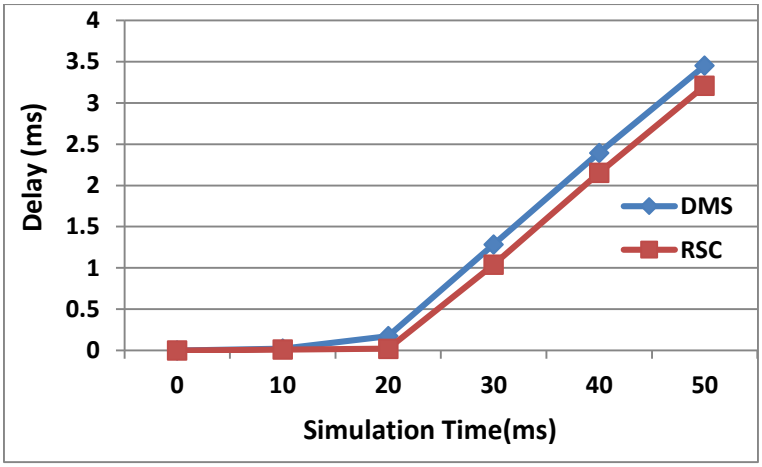

Figure 6: Average Delay

4.5 Residual Energy

The amount of energy remaining in a node at the current occurrence of time is called as residual energy. The energy efficiency is shown in the figure 7 below.

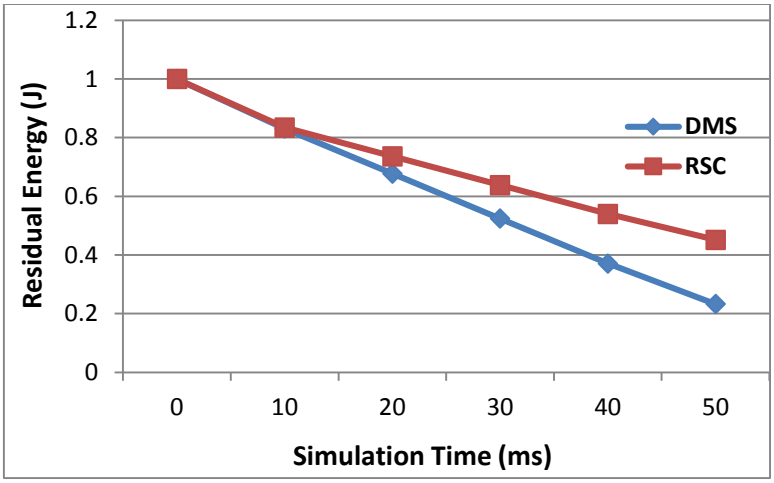

Figure 7: Residual Energy

It shows that RSC grants greater residual energy when compared to the existing protocol.

V. CONCLUSION

This paper proposes Revival of Selfish nodes in clustered MANETs to encourage cooperation of the selfish node with the other nodes. A node generally behaves selfish in order to save its energy. When data transmission occurs, and when the energy of the node is below threshold, the base station automatically adds the energy. This process is monitored by selfish node and revival of selfishness then co-operates all nodes in the networks. Simulation results show that the proposed method has low packet loss ratio, packet delay and better packet delivery ratio, residual energy and throughput.

VI. FUTURE WORK

In recent years many research works are doing Cognitive Network. It features are adaptive, robust communications, distributed resource management and self configuration. In future, the Revival of Selfish nodes in clustered performed in Cognitive Networks.

REFERENCES

[1] Samreen, S.; Narasimha, G., "An efficient approach for the detection of node misbehaviour in a MANET based on link misbehaviour," *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, vol., no., pp.588, 592, 22-23 Feb. 2013.

[2] Talreja, R.; Jethani, V., "A vote based system to detect misbehaving nodes in MANETs," *Advance Computing Conference (IACC), 2014 IEEE International*, vol., no., pp.391, 394, 21-22 Feb. 2014.

[3] Hernandez-Orallo, E.; Serrat, M.D.; Cano, J.-C.; Calafate, C.T.; Manzoni, P., "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog," *Communications Letters, IEEE*, vol.16, no.5, pp.642, 645, May 2012.

[4] Djenouri D and N.Badache, "New approach for selfish nodes detection in mobile ad hoc networks," In Proceedings of the Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005., vol., no., pp. 288- 294, 5-9 Sept. 2005.

[5] Kargl F., A. Klenk, S. Schlott, and M. Weber, "*Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks*", In Proceedings of the 1st European on Security in Ad-Hoc and Sensor Networks (ESAS 2004) Heidelberg, Germany, August 6, 2004.

[6] Hussain, M.A.; Nadeem, A.; Khan, O.; Iqbal, S.; Salam, A., "Evaluating network layer selfish behavior and a method to detect and mitigate its effect in MANETs," *Multitopic Conference (INMIC), 2012 15th International*, vol., no., pp.283,289, 13-15 Dec. 2012.

[7] Hernandez-Orallo, E.; Olmos, M.D.S.; Cano, J.; Calafate, C.T.; Manzoni, P., "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes," *Mobile Computing, IEEE Transactions on*, vol.14, no.6, pp.1162, 1175, June 1 2015.

[8] Manchikalapudi, V.; Yelisetti, S.; Surapaneni, R., "Detecting misbehavior nodes and trust levels in manets," *Engineering Education: Innovative Practices and Future Trends (AICERA), 2012 IEEE International Conference on*, vol., no., pp.1,4, 19-21 July 2012.
[9] Muthumalathi, N.; Raseen, M.M., "Fully selfish node detection, deletion and secure replica allocation over MANET," *Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on*, vol., no., pp.413, 415, 3-3 July 2013.
[10] Rachedi, A.; Badis, H., "MIMODog: How to solve the problem of selfish misbehavior detection mechanism in MANETs using MIMO technology," *Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International*, vol., no., pp.333, 337, 27-31 Aug. 2012.
[11] Tarannum, R.; Pandey, Y., "Detection and deletion of selfish MANET nodes-a distributed approach," *Recent Advances in Information Technology (RAIT), 2012 1st International Conference on* , vol., no., pp.152,156, 15-17 March 2012.
[12] Sundararajan T.V.P.,A.Shanmugam, "Modeling the Behavior of Selfish Forwarding Nodes to Stimulate Cooperation in MANET" International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010.
[13] Sujit Kumar Das, Pinaki Sankar Chatterjee, Monideepa Roy, "Detecting and Punishing the Selfish Node and its Behavior in WSN", International Journal of Computer & Organization Trends – Volume 6 Number 1 – Mar 2014.
[14] Dipali Koshti, Supriya Kamoji, "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", International Journal of Soft Computing and Engineering (IJSCE) Volume-1, Issue-4, September 2011.

AUTHORS BIOGRAPHY

Santhosh Kumari received her Bachelor's Degree in Electronics and Communication Engineering from GPR college of Engineering affiliated to Anna University in 2005, Chennai, India and her post graduation was M.Tech in Applied Electronics from Dr. MGR University, Chennai, India. She has been working an assistant professor at Ganadipathy Tulsis Jain Engineering college, Velloor, India. She is working towards her research in the field of Mobile Ad hoc Networks. Her field of interest includes Wireless Networks and Telecommunication.

K. Thirunadana Sikamani has been working as Professor & Head, Department of Computer Science & Engineering, St. Peter's College of Engineering & Technology, Avadi, Chennai, India.