International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

# Intrusion Detection Algorithm for Packet Loss Minimization in Wireless Sensor Networks

**S. Rizwana, Gayathri. K M, Thangadurai N**

***Abstract:*** ***Wireless Sensor Network consists of a greater number of sensor nodes and recent advance is in wireless communications and it serves a backbone for controlling the real time applications. It consists of group of sensor nodes and that is sense the information from the event area and it is passes through the base station and which it reacts according to environment and to provide a large-scale monitoring and sensor measurement in a high temporal and the spatial resolution. The researcher uses a different algorithm in that they use a distributed energy fuzzy logic to reduce a packet loss. Wireless Sensor Networks are unprotected to many kinds of the security threats which can decrease the performance of network and cause the sensors to send wrong data to destination. The hostile node in the network is working as an attacker node and it takes all the information packets which is delivered through them. In this paper we propose an intrusion detection system algorithm against the packet dropping. Intrusion detection algorithm solves the problem by analyzing the network by detecting the abnormal node. Then the abnormal node is corrected into normal node with the help of intrusion detection algorithm.***

***Index Terms*: *Intrusion Detection algorithm, Network Security, Packet dropping, Distributed Energy Fuzzy Logic***

## I. INTRODUCTION

Wireless Sensor Network is a dispersed network, which has the huge number of network nodes, self-directed and small in size. It is encompassing the large number of the spatially dispersed and the networks are supportive with the sensor nodes to collect the data then process with the routing protocol to convey data to the base station and they make a connection with one another in a various topology to archive the maximum performances [1]. Wireless Sensor Network have a number of sensor nodes that can be in order of hundreds or thousands. Due to advancement in wireless communications the low cost, low power and the multi-functional sensors are available. These are in the small dimensions and communicate with short distances and these low cost, smart sensor are networked through the wireless links. Then it is deployed in the huge quantities to provide the precedented opportunities for observing and controlling sensors along with the environment and the networked sensors are used in the broad spectrum for the applications with the defense area and generating a new capability for the surveillance of various applications [2-4]. Self-localization is the capability that can be a greatly desirable sign for the wireless sensor networks. The environmental observing applications such as quality of water monitoring and precision agriculture etc measure the information with the lacking of knowledge to the place in the location and where the data is obtained and the location is estimated with many applications they are intrusion detection such as health monitoring, road traffic monitoring, etc and all the advances is inside the miniaturization and the integration of the sensing and the communication technologies with the large scale WSN. Wireless Sensor Network sends the information to the base station without security and many securities are used in WSN with the secure routing for a specific attack. The instruction detection system is one of the possible solutions to make an extensive range of security with attacks in WSN. The intrusion detection system can detect the attacks and recovery. If the attack is detected means the algorithm will inform to the controller to take an action. There are two types of intrusion detection system namely 1) rule-based IDS and 2) anomaly-based IDS. Rule based IDS is a signature-based IDS and it is used to detect the infringement with the help of the in signatures and it also detect the attacks with the greater accuracy but it is tedious to recognize the fresh attacks for the signatures that are not there in the intrusion database [5-6]. Anomaly based IDS detect the disturbance by the traffic patterns with the resource utilizations and it have been a ability to detect the new attacks and it is operate in a routing protocols and to implemented on the every node so then only all the nodes are cooperate to detect the routing intrusions and the nodes are sense into the region for the occurrence at the event in a different locations and it passed into the sensed information to base station node so that it is react according to the condition. The topology of WSN is refer to the arrangement of nodes within the network. WSN consists of sensors that are coordinated. The general principle of topology of WSN are the same for another network. The topology of WSN includes various topologies given [7-8]. In Star topology each node connects directly connect to the gateway. An individual gateway can transmit and receive information to a number of remote nodes [9-10]. The sensor node has a restricted amount of processing and it is coordinated with message of the other nodes and they have an ability to calculate a actual nature to carry out a task with a complex function and the network is described a gathering of sensor nodes and that is coordinate with each other to execute a specific actions. Before transmission the sensor nodes are process with the raw data and help to build in the processor to include in the nodes itself to sensing the computation and the communication of the capabilities and it is highly used in the large number of different applications and the security attacks in.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

**S. Rizwana*,** PG Scholar, Department of Electronics and Communication Engineering, School of Engineering and Technology, JAIN (Deemed-to-be University), Bangalore, Karnataka, India

**Gayathri. K M**, Department of Electronics and Communication Engineering, School of Engineering Technology, JAIN (Deemed-to-be-University), Bengaluru, Karnataka, India

**Thangadurai N,** Department of Electronics and Communication Engineering, School of Engineering Technology, JAIN (Deemed-to-be-University), Bengaluru, Karnataka, India

WSN are categorize in to two ways they are active and passive attack and the active attack is the simplified processing capabilities and it has a restricted power resources to use them into a number of other possible attacks and second is the network connectivity to the external world without any inbuilt protection [11-12]. Detecting is used to select the packet dropping attacks is an extreme challenge in a wireless environment and the requirement to recognize the place where the packet is falling and also identify the drop is predetermined or not due to the open nature of the wireless medium with the packet lost in the network could be caused by the channel situation they are noise, interference, link errors, insider attacker and two categories are explained they are internal and outside attack and the external attack is instigate by the node. It does not belong to the network and this attack is to cause the congestion in network then it is spread the incorrect routing information and the inside attack is due to the hostile internal node then the defense strategies and it is generally aim to protect the network against the external attacks and the internal attacks is the most of the significant threats that can be interfere in the WSN [13-15].

## II. PROPOSED WORK

Distributed energy fuzzy logic algorithm is assigning to energy related to cost values in the network links and utilizes the minimum distance path strategies to detect the set of routes with the total path cost from source to sink. The network lifetime performance for the distributed energy fuzzy logic is also reduced because of the packet loss and it is not used a security. The proposed algorithm is an intrusion detection algorithm which is based in the gathering and analysis the system to network information and it is used for detection, intrusion and it should be reported to the security management and it is constantly monitors the activities like a packet traffic. Each mobile node runs in IDS and independently to observe the operation of the neighboring nodes and making the decision to prevent a system from the attack then it can also request for the data and the actions from the neighboring nodes. Intrusion detection system consist of the network-based ID and host-based ID. Identifying attacks and the hostile actions are done with respect to neighboring nodes with their coordination between each other and it runs on the gateway of the network and it is acquired message from the traffic and then it is analyzed the data gathered and host based intrusion detection is acquires the data through the files that run on the node.

The combination of the network-based intrusion detection and the host-based intrusion detection can be used to find the attacks and it makes a powerful distributed IDS system then the message packs are transmitting in the network then the data are gathered from the network nodes with the basis of the intrusion detection. To reduce the effect of the packet, drop in the node to improve the performance of the network. The node sends the request response message without checking the route then with the help of the dynamic source routing and it will check a route response packet from the node for the minimum path to the destination then it chooses the maximum destination of the sequence number. The intrusion detection system in dynamic source routing Protocol will give the route response packet from the node and choose the next coming route response packet from the sink. These protocols maintain the consistent with up to date routing message in network and then the nodes send the routing with the data regularly when there is an even small difference in the network configuration and each node keeps one or more connecting table to reserve the connecting data in every other node to the network. Some network is avoid a lot of the message then it will create the delay and congestion in network but in M-Leach it use a many node to transmit more message in the network and it evolves the periodic transmission even when there is a no change in the node position and this is the simply reduce the network resources. It is used to find the route between the source and the destination and it is allow the nodes to obtain the latest paths for a current sink and the data are used to observe and detect the links to the neighbors in every node and send periodically in a broadcast to the neighbors node and the packet transmission is failed. Hence IDS used to create the path to the sink to achieve the source node to send a requested data.

First start the network then initialize the node and start the transmission to send the packet to the node and that time some packet is dropped means attack is occur in that network so use a intrusion detection system to change the abnormal node into normal node.

When the source is received the message means the destination is ready to accept the message and route is working properly in the network. The source node is the first broadcast route request packet to all intermediate nodes then after receive the route request packet in the intermediates nodes maintains the reverse route and it contain the sender's information. Then the nodes start the falling packets that means its stop and forwarding the packet to the next node.

The hostile node is a insider attack and it is attack the network and it can analyze the importance to transmitting packet and control the performance of the network and if the attacker is continuously dropping the packets and it can be detect easily. If the malicious node is unknown means one can use a randomized multipath routing of M-LEACH to circumvent the packet drop holes are created by the attack. Every packet in WSN contain a distinctive sequence of number and this number is rising the value and it is consequent packet and have a higher value to present the packet in sequence number. The node is in a regular routing protocols to contain the last packet in the sequence range that it is received and used to examine the received packet whether it is received before from the identical and the originating source. Intrusion detection system in each node must have the two extra small sized and the last packet in sequence numbers in a different way of route. The nodes are updated once any packet is arrived that exists in a dynamic source routing network then announce itself having the valid route to the destination node then the next one is the node drops and it is controls all the intercepted
packets and this attack sending route request messages and to detect the attacks they are set the originator with the route request and create the destination in route request. The M-Leach protocol flow chart is given in fig 2.

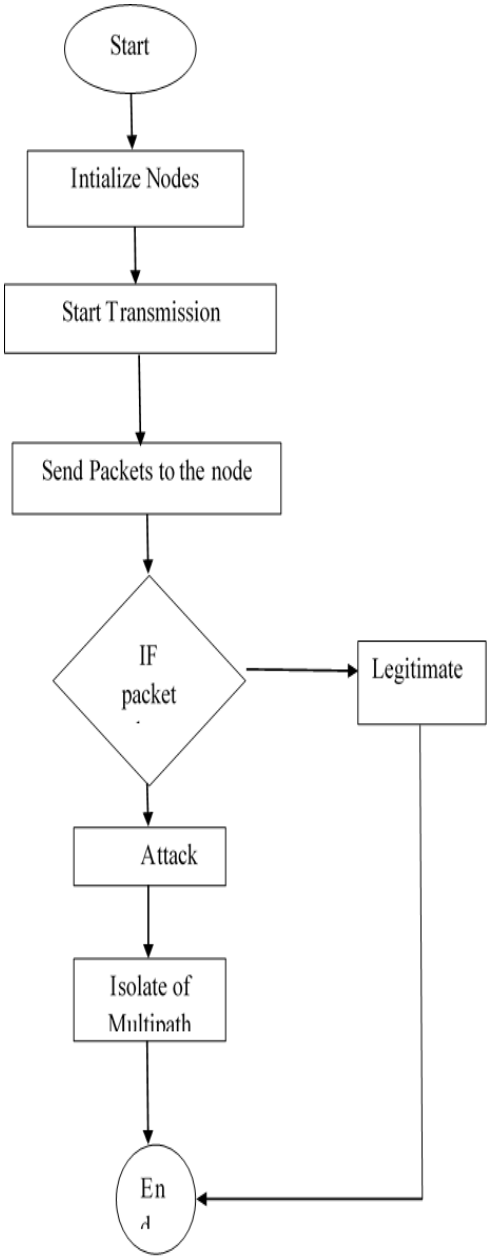


**Fig.1. Packet drop**

First initialize the node and choose the cluster head based on the shortest path and the another cluster member are send the information to the cluster head then the cluster head send the information to the base station or if the cluster head is not selected then more energy losses is occur .The cluster head is selected at a time in the cluster member in group. M-LEACH is the most popular energy-efficient for clustering in WSN that is proposed for minimizing the power consumption, prolong network and the clustering task is revolved among the nodes and it is based on the duration.

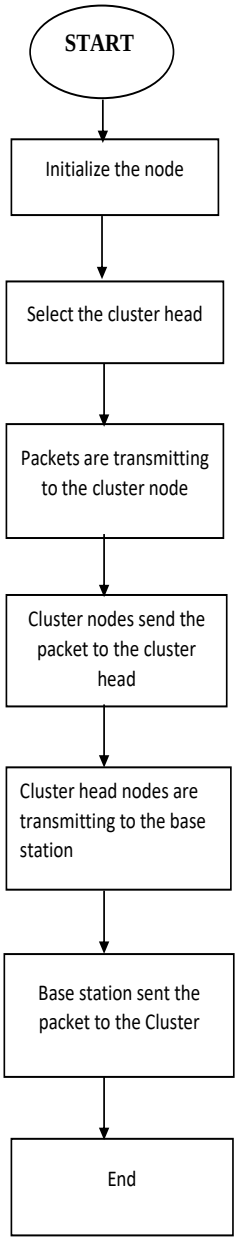


**Fig.2. .M-LEACH**

The communication is used by each CH to forward the information to the base station. It is based on the aggregation that is combines on the original data into the smaller size of the data to carry only the meaningful information of all sensors. It is dividing the network into a several cluster of the sensors and which is developed by using the localized coordination to control not only reduce an amount of data are sent to the destination and also, make the routing and information dissemination are the more scalable and robust.

## III. RESULT AND DISCUSISON

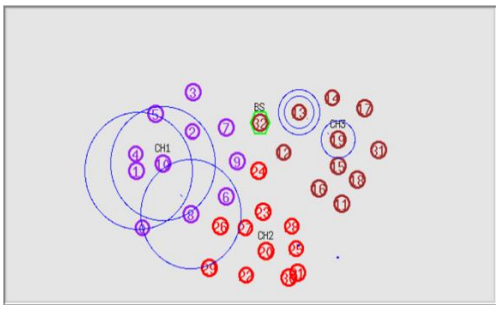


**Fig.3. Nam Window**

In NAM window 32 nodes are created and give a traffic agent, data transmission etc. The 31 nodes are separated into 10 cluster members in that select the cluster head based on the shortest path interval to the base station.Packet drop is occurred because of the malcious attack then the attacker is attacking the node with the packet drop and it is denoted as a abnormal node. The abnormal node are fourth, twenty and fifteen from the cluster head 1, cluster head 2 cluster head 3 and the seventh node from the cluster head 1 nodes is transmit to the base station and then base station transmission is occur to send the data to other nodes.

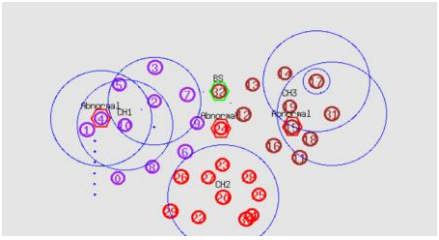


**Fig.4. Abnormal node**

Then the abnormal nodes are changed into the normal node with the help of the intrusion detection system.

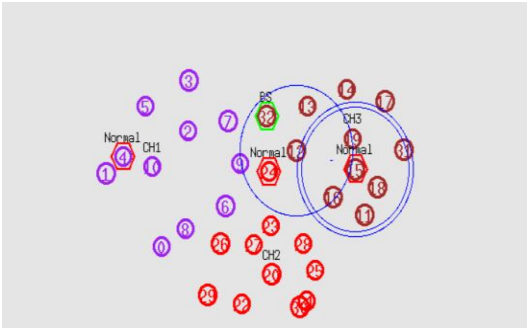


**Fig.5. Normal node**

### 5.1 Throughput Analysis:

The overall packet is transmitting in the network in 3 second is 100 percentage and then the proposed consist of 100 packets is compare with the existing system. The distributed energy fuzzy logic is consisting of 50 packets in that 20 packets only transmitted in 12 seconds.

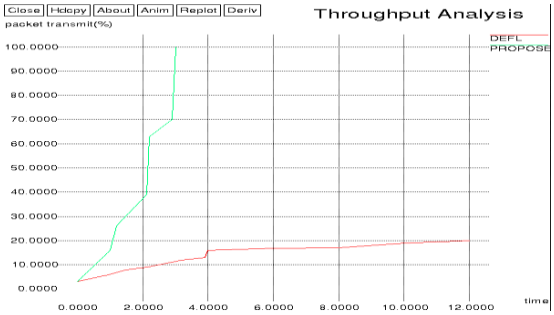


**Fig.6. Packet Transmitted**

Then overall packet is received in the proposed system is 90 percentage for 100 packets in 4 seconds and it is compared with the distributed energy fuzzy logic in that only 20 percentage of packet is received for 50 packets in 12 seconds.

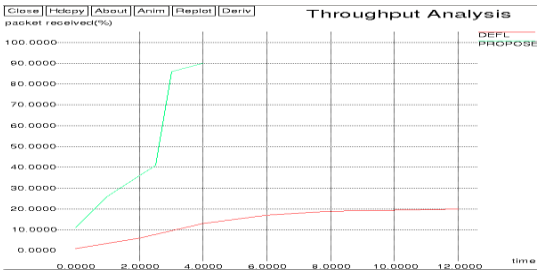


**Fig.7 Packet Received**

In this proposed system packet drop is occur because of the malicious attack so in the proposed system packet drop is occur for three node that is 50 percentage without using intrusion detection system and after using a intrusion detection system 40 percentage of packet is recovered in 10 seconds.

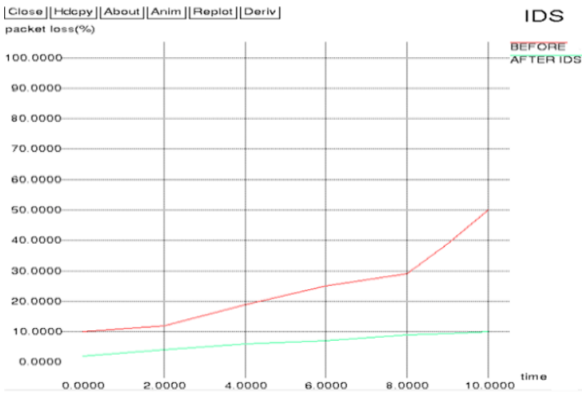


**Fig.8 Intrusion Detection System**

**Table1 Comparison Of Number Of Packets With And Without IDS**

| Node | Number of Packet loss without IDS | Number of Packet loss with IDS |
|---|---|---|
| 4 | 15 | 2 |
| 24 | 18 | 3 |
| 13 | 17 | 1 |

In this proposed system cluster head 1 has a fourth node and that is attacked with the packet loss of 15 percentage without using ids then the packet loss is reduced 4 percentage with ids then cluster head 2 has a 24 node and that is attacked with the packet loss of 18 percentage without

using ids then the packet loss is reduced 4 percentage with ids at last cluster head 3 has a 13 node and that is attacked with the packet loss of 17 percentage without using ids then the packet loss is reduced 2 percentage with ids.The packet losses are comparing with the existing system and proposed system. The proposed system has a 10 percentage of packet losses in 10 seconds and in the distributed energy fuzzy logic 30 percentage of packet is losses in 12 seconds.

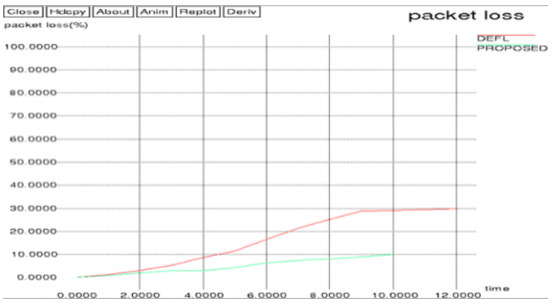


**Fig.9. Packet loss vs Time**

The delay is in the proposed system is 20 percentage in 10 seconds and it is compare to other algorithm this proposed algorithm is extend the network lifetime.

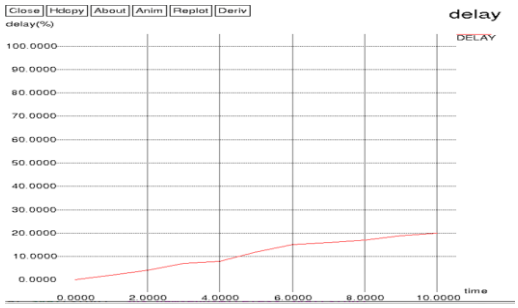


**Fig.10. Delay vs Time**

## CONCLUSIONS

The wireless sensor networks is made up of a sensor nodes that can observe the environmental conditions and the sensed information will be passed to base station and the number of sensor vertex is very small and it is self-configuring of the network due to the hostile nodes and because of the packet loss occur in the network and the proposed ids is used to identify and distinguish the hostile nodes from the network and the proposed algorithm is reduce the packet loss compared to the available algorithm and the proposed algorithm is improve the network performance. The future work is comparing with the detection rates and the detection ratio that is true positives and false positives values in each node and examine the performance with the various set of the simulation framework.

## REFERENCES

1. Vivek Katiyar Narottam Chand Surender Soni" Improving Lifetime of Large-scale Wireless Sensor Networks through Heterogeneity" ICETECT 2011
2. H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. Hanzo, "A survey of network lifetime maximization techniques," IEEE Communication Survey. Tut., Vol. 19, no. 2, pp. 828–54, Jan. 2017.
3. G. Anastasi, M. Conti, M. D. Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," Ad Hoc Networking, Vol. 7, no. 3, pp. 537–68, May 2009.
4. C.-W. Tsai, T.-P. Hong, and G.-N. Shiu, "Metaheuristics for the lifetime of WSN: A review," IEEE Sensors Journal, Vol. 16, no. 9, pp. 2812–31, May 2016.
5. N. Thangadurai and Dr.R.Dhanasekaran, "Energy Efficient Cluster based Routing Protocol for Wireless Sensor Networks", International Journal of Computer Applications, Vol. 71, No. 7, pp. 43-48, 2013.
6. Z. Lu, W. W. Li, and M. Pan, "Maximum lifetime scheduling for target coverage and data collection in wireless sensor networks," IEEE Trans. Vehicle Technology, Vol. 64, no. 2, pp. 714–27, Feb. 2015.
7. N.Thangadurai, Dr.R.Dhanasekaran and R.D.Karthika, "Dynamic Traffic Energy Efficient Topology based Routing Protocol for Wireless Ad hoc Sensor Networks", International Review on Computers and Software, Vol. 8, No. 5, pp. 1141-1148, 2013. (Scopus Indexed)
8. V. C. Manju, S. L. S. Lekha, and M. S. Kumar, "Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks," in IEEE Conference on Information & Communication Technologies (ICT), pp. 74-77, 2013.
9. E. B. Ram Pradheep Manohar, "Detection of Stealthy Denial of Service (S-DoS) Attacks in Wireless Sensor Networks " International Journal of Computer Science and Information Security (IJCSIS), vol. 14, pp. 343-348, 2016.
10. Kavitha T, Muthaiah R, "Mitigation of Blackhole Attack using Neighbour Coverage", International Journal of Mechanical Engineering and Technology, 8(8), 2017.
11. N.Thangadurai, Dr.R.Dhanasekaran and R.D.Karthika, "Dynamic Energy Efficient Topology for Wireless Ad hoc Sensor Networks", WSEAS Transactions on Communications, Vol. 12, Iss. 12, pp. 651-660, 2013. (Scopus Indexed)
12. G. Mahalakshmi, P. Subathra, "Denial of Sleep Attack Detection Using Mobile Agent in Wireless Sensor Networks", International Journal for Research Trends and Innovation, Volume 3, Issue 5,2018
13. Jinyuan Sun ,Chi Zhang ,Yanchao Zhang ,Yuguang Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks", IEEE Transactions on parallel and distributed system, vol 21, no.9, pp.1227-1239, 2010.
14. Sarita Agrawal , Manik Lal Das," Detection of Node Capture Attack in Wireless Sensor Networks", IEEE Transactions on parallel and distributed system, , vol 30, 2018.
15. Shalu Malik, Anil Kumar Sharma, "Detection and Isolation Techniques for Blackhole Attack in Wireless Sensor Network" International Journal of Computer Engineering & Technology Volume 9, Issue 1, Feb 2018.

## AUTHORS PROFILE

**Rizwana S** is a PG Scholar in the department of Electronics and Communication Engineering, Jain(Deemed-to-be University), Bangalore. She has obtained her bachelor's degree in Electronics and Communication Engineering from K.Ramakrishnan College of Technology, Tamilnadu in the year 2017. She has pursuing her Master's Degree in Embedded System Design at Jain Jain(Deemed-to-be University), Karnataka. Her areas of interest in Wireless Communication and Embedded System Design.

**Gayathri K M** is an Assistant Professor in the Department of Electronics and Communication Engineering, School of Engineering and Technology, Jain (Deemed-to-be University), Bangalore. She has obtained her Bachelor's Degree in Medical Electronics and Master's Degree in VLSI and Embedded Systems. Awarded PhD in 2018 from Jain University. She is having 8 years of teaching experience and 4 years of industry experience. She has published 13 research papers in both International and National Journals and presented papers in conferences. She has guided UG and PG students for their academic projects. Her areas of interest are VLSI, Wireless Communication, Satellite Communication and Navigation Systems. She is working as Principle Investigator for ISRO funded projects. She is also an associate member of OSI and IEEE.

**Thangadurai. N** is working in Department of Electronics and Communication Engineering, Jain (Deemed-to-be University) Bangalore. He has obtained his Ph.D Degree in Wireless Sensor Networks, Bachelor's Degree in Electronics and Communication Engineering and Master's Degree in Applied Electronics. He has published more than 100 research papers in both International and National Journals and conferences. He has supervised 60 numbers of undergraduate and postgraduate students for their project completion and guiding 6 Ph.D., scholars now.

He is currently working with sponsored research project grant received from ISRO. He has also filed 13 Indian patents into his credit. His research interests are Networking, Wireless Communication, Satellite Communications, Mobile Adhoc and Wireless Sensor Networks, VANET, Embedded Systems, Optical Communication, and Navigation Systems. He is also a Life member of following professional bodies like ISCA, ISTE, IAENG, and IACSIT. Also he is a fellow of IETE and OSI. He has received many awards like Award for Research Publications from VGST 2016-17, Bharat Excellence Award -2017, Outstanding Researcher Award – 2016