International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.3, No.12, December 2014 DOI:10.15693/ijaist/2014.v3i12.110-115

An Energy based Load Balanced Routing Scheme for Wireless Sensor Networks

Harikrishnan G
Assistant Professor,
Department of Electronics and communication Engineering
Nirmala College of engineering
Chalakudy Kerala

Abstract – In Wireless Sensor Networks, Sensor nodes are controlled by either base station or without bases station. In our scheme, the sensor nodes are not depends on the base station. Once the sensor node sent a packet to the destination node, the residual energy is calculated through the multipath routing approach. There is a need of Secure and Energy based Routing in the wireless sensor network. This requirement may lead to a number of routing protocols which effectively use the limited resources available at the sensor nodes. Many routing protocols will attempt to find the efficient and secure multipath routing. In order to determine the secure and energy efficient routing, we proposed the Residual Energy based Multipath Routing Approach (REMRA) which attains the integrity and minimum residual energy. It consists of three phases. In first phase, the concept of multipath routing is proposed. It uses load balancing to prevent congestion problems in the network. In second phase, the path stability is established based on link cost, link quality, link bandwidth and load balancing. In third phase, the energy residual consumption model is proposed. By simulation results, the proposed REMRA achieves better delivery ratio, throughput, less delay and energy consumption in terms of mobility, time and number of nodes than our proposed scheme NMRA and existing scheme SByaoGG.

Keywords –Energy Consumption, Data delivery ratio, mobility, time, Congestion, Load Balancing, throughput and link quality, multipath routing and WSNs.

I. NTRODUCTION

A. Wireless Sensor Networks (WSNs)

The current technological advancement has already come to terms with immense potential of Wireless Sensor Network, Which consists of tiny sensor nodes scattered in a region communicating with each other over well defined protocols and transferring information of temperature, humidity etc between each other. Compared to ad hoc networks, sensor networks have some unique feature and application requirements.

Wireless sensor network generally composed of a large number of distributed sensor nodes that organize themselves into a multi-hop wireless network. Each network is equipped with more than one sensors, processing units, controlling units, transmitting units etc. Wireless sensor networks (WSN) are now used in many applications including military, environmental, healthcare applications, home automation and traffic control. It consists of a large number of sensor nodes, densely deployed over an area.

B. Security goals and threats of Wireless Sensor Networks WSNs)

Based on the application, different architecture, goals and constraints have been considered for WSNs.

Security Threats:

A. Eavesdropping

Eavesdropping occurs when an attacker compromises an aggregator node and listens to the traffic that goes through it without altering its behavior. Since aggregator nodes process various pieces of data from several nodes in the network, it does not only leak information about a specific compromised node, but from a group of nodes.

B. Data tampering and packet injection

A compromised node may alter packets that go through it. It may also inject false messages. Since an aggregate message embeds information from several sensor nodes, it is more interesting for an attacker to tamper with such messages than simple sensor readings. An attacker that controls the meaning of the malicious messages it sends may heavily impact the final result computed by the sink.

C. Denial of service (DoS)

A compromised node may stop aggregating and forwarding data. Doing so, it prevents the data sink from getting information from several nodes in the network. If the node still exchanges routing messages despite its unfair behavior, that problem may be difficult to solve. Smarter attacks also involve dropping messages randomly. It is also difficult to detect when an attacker sends garbage messages.

Problem Statement:

In wireless sensor networks, the sensor nodes are attacked by several attacks like eavesdropping, data tampering, false packet injection and denial of service attack. When the source node sends a packet to destination node, the intruder may eavesdrop the message that is carried by packet. Some intruders may cause the misrouting, false packet injection and packet lost. Because of the incorrect path stability, the intruders may arise and misuse the information. So the retransmission will occur unnecessarily. Thus the node consumes more energy after packet sending and receiving period. In this research work, we focus on remaining energy

based multipath routing scheme. Here node occupies more energy after the packet sending and receiving period. To avoid the retransmission, we focus on the path stability and multipath approach. So the sensor node will have more energy consumption. To reduce the effects of eavesdropping, data tampering, false packet injection and denial of service attack, the stability of path is undertaken here. In addition to this, we calculate the residual energy of the sensor node once the packet loss or discard or any bad packet error sent or received. This calculation determines the efficiency of our proposed scheme.

II. RELATED WORK

Senthil kumar et.al [1] analyzed the base station which is used to provide individual base station attacks or sensor node compromises problem to design a sensor network routing protocol that satisfies the proposed security goals. One aspects of sensor networks organized hierarchically, with a base station serving as a gateway for collecting data from a multi-hop network of resource-constrained sensor nodes.

Sabarinathan et.al [2] proposed approach mechanisms that generate randomized multi-path routes, even if the routing algorithm becomes known to the adversary, the adversary cannot pinpoint the routes traversed by each packet. Besides randomness, the generated routes are also highly dispersive and energy efficient, making them quite capable of circumventing black holes. Instead of splitting message into shares, here splitting message into packets and applying MD5 algorithm to provide additional security. The proposed approach provides confidentiality, minimize packet interception probability and end-end energy consumption, the additional features provide solutions to cut-around sink attack.

Shuang Li et.al [3] proposed a multipath based on directed diffusion that reinforces multiple routes with high link quality and low latency. This algorithm retains the merits of the original directed diffusion algorithms, including its energy efficiency and scalability. A hybrid metric of link quality and latency is used as the criterion for path selection. In order to select disjoint paths, we propose a scheme for reinforced nodes to respond negatively to multiple reinforcement messages. They used the NS-2 simulation tool with video trace generated by Multiple Description Coding (MDC) to evaluate the performance. The results show that our algorithm gives better throughput and delay performance, i.e higher video quality, than standard directed diffusion that transmits over a single path, with low overheads and energy consumption.

Hamid reza Hassaniasl et.al [4] proposed Score-Aware Routing Algorithm (SARA) is used to enhance routing quality. For that, they have analyzed the five factors like distance between each node and sink, number of observed sources by each node, remaining energy in each node and reliability of communication link and value of traffic in each node. It was more efficient in terms of decreasing delay, decreasing the number of lost packets, improving the load distribution and purposeful network lifetime. It was shown that with higher network density or higher number of sources and higher rate of sent data, the efficiency of the developed algorithm would increase, and such increase is due to the higher number of nodes suitable for selection for routing.

Yuxin Mao and Guiyi Wei [5] proposed a novel approach of secure data collection for wireless sensor networks. They explored secret sharing and multipath routing to achieve secure data collection in wireless sensor network with compromised nodes. They presented a novel tracing-feedback mechanism, which makes full use of the routing functionality of wireless sensor networks, to improve the quality of data collection. The major advantage of the approach is that the secure paths are constructed as a by-product of data collection. The process of secure routing causes little overhead to the sensor nodes in the network. Compared with existing works, the algorithms of the proposed approach are easy to implement and execute in resource-constrained wireless sensor networks.

S. Saqaeeyan and M. Roshanzadeh [6] proposed optimum routing protocol, in some of Quality of Service achieved improvements in the field of reliability in data sending to destination and load balancing in wireless sensor network. In the proposed protocol, to ensure that a data packet correctly send to the destination, it used of an improved hybrid method based on multipath data sending. The routing decisions in this method are by considering the remaining energy of nodes that are in neighbors of sender nodes.

Riyaz Pasha et.al [7] presented model of self-optimized multipath routing algorithm for WSN and its results. mechanism is based on delay, energy and velocity. The adopted factors and reinforcement learning (RL) feature help WSN in improving the overall data throughput; especially in case of real time traffic. The algorithm is also capable to avoid permanent loops which promotes dead lock problem in the running networks. The dead lock problem is cured by assigning unique sequence ID to every forward ANT and also to search ANT.S. Ganesh and R. Amutha [8] developed a comprehensive approach to understand the fundamental performance of information routing in energy-limited wireless sensor networks through optimal Signal to Noise Ratio (SNR) based power control mechanism and optimal handoff-based self-recovery features. They presented some results for a few different small-scale WSN experiments to study the solutions obtained for these problems.. They found that

higher fairness constraints can result in significant decrease in information extraction and higher energy usage. Another observation about the results is that the flow and energy curves show qualitatively abrupt changes as the fairness constraints are varied. Based on the simulation results, they concluded that efficient and secure routing protocol (ESRP) with optimal power control mechanism and handoff-based self-recovery can significantly reduce the power usage.

Reza Azarderskhsh and Arash Reyhani-Masoleh [9] proposed a new secure clustering scheme for clustered WSNs incorporating public key cryptography. They take an advantage of gateway nodes which are powerful and tamper proof to establish/revocate the symmetric keys in each cluster. This key establishment is completed during the bootstrapping and clustering phase assuming that the adversary is present in the field.

S. Saqaeeyan and M. Roshanzadeh [10] presented the reliable and energy aware packet delivery mechanism to ensure quality of service in wireless sensor networks. In the proposed algorithm to ensure that a packet of information sent to the destination, the multi-path forwarding method is used; So that several copies of an information packet via separate routes are sent to the destination, also routing decisions in this way occurs by considering the remaining energy in the neighborhood of nodes that are located in two hop of sender node.

Jayashree et.al [11] analyzed the delay and energy problem in the routing based on the clustered and multi sink WMSN attributes. They proposed a multi-sink wireless sensor network architecture where the network is partitioned into clusters with multiple sinks to increase the manageability of the network and also to reduce the energy dissipation at each node. All the sources in a cluster were assigned to send the video and imaging data to the sink designated to that particular cluster in order to ensure efficient usage of the loss at each node. This protocol prevents packet clustering and provides smoothness to the traffic. Through monitoring and controlling the scheduling rate the flow control and congestion control are managed.

Venkata Sumanth Mareedu et.al [13] proposed Concentrated Dissimilate Algorithm, a very simple algorithm that strengthens the reliability of spreading in such networks. The algorithm requires only limited information, and resides as a service between

S.Pratheema et.al [14] explored the multipath routing the data over the path proposed scheme helps to reduce the probability that communication is disrupted and data is lost in case of link failuresthe MAC layer and network layer, taking information from both. It is shown that Concentrated Dissimilate Algorithm improves reliability at the same time balancing energy efficiency.scheme distribute traffic among multiple paths instead of routing all the traffic along a single path and in case of link failure and retransmission alternate path is chosen to flow

.

sensors and effective access to the gathered information. The proposed protocol ensures end-to-end delay requirement of real time data, as well as maximizes the throughput of non real-time data by transmitting the gathered data to the appropriate sink.

Mary Cherian and T. R. Gopalakrishnan Nair [12] proposed multipath routing algorithm which enables the reliable delivery of data. The congestion and packet loss are prevented in the network using scheduling rate control. The algorithm provides an efficient way to prevent the packet

Tapiwa et.al [15] proposed the new distributed topology to enhances the energy efficiency and radio interference to preserve the global connectivity. The drawback of the approach is lack of balancing the energy consumption and security. It does not provide better authentications to the information carried by the packets. To overcome this issue, our scheme enhances the multipath routing to achieve better data authenticity and attains the correct balance between the energy consumption and security.

K. Vanaja and R. Umarani [16] deals with the fault management to resolve the mobility induced link break. The proposed protocol is the adaptive fault tolerant multipath routing (AFTMR) protocol which reduces the packet loss due to mobility induced link break. In this fault tolerant protocol, battery power and residual energy are taken into account to determine multiple disjoint routes to every active destination. When there is link break in the existing path, AFTMR initiates Local Route Recovery Process.

III. IMPLEMENTATION OF PROPOSED ALGORITHM

Our proposed Multipath routing scheme consists of concept of proposed multipath routing, determination of path stability, load balancing, remaining energy and secure routing in multipath to provide the security and improve energy efficiency in sensor networks.

A. Concept of Proposed Multipath Routing

The concept of proposed multipath feature is towards broadcasting the traffic load among two or more routes. Load delivery is to avoid the congestion problems in the network and to increase data throughput rate. The proposed multipath system in figure1 uses multi-path routing in order to select the route with the best maximum data throughput rate.

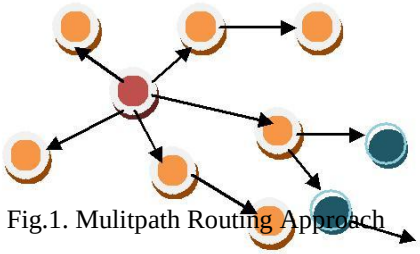

Fig.1. Mulitpath Routing Approach

B. Determination of Path Stability

In order to reduce the effect of DoS attacks, Data tampering and Eavesdropping, the stability of path is undertaken here. Path stability includes the link cost, link quality and bandwidth of the link. The link cost function is used by the node to select the next hop during the path search phase. Let N_b denote the neighbor set of node b, node b will choose the next hop by following the criterion.

$$L_{ct} = \arg\min_{l \in N_b} \left\{ \left(1 - \frac{e_{j,remaining}}{e_{j,init}} \right)^{[\delta (1 - \frac{(\Delta dh+1)}{d})]} \right\} \quad (1)$$

where d_{oe} is the distance in hops between node o and sink e; d_{ke} is the distance in hops between node k and sink e; dh is the difference between d_{oe} and d_{ke}; $e_{j,init}$ is the initial energy level of node j; $e_{j,remaining}$ is the remaining energy level of node j; and δ is the weight factor and $\delta > 1$. Note that $(\Delta dh+1) \in \{0, 1, 2\}$ and $(1-e_{j,remaining}/e_{j,init}) \in [0, 1]$. The link cost function takes both the node energy level and hop distance into account. Suppose $e_{j,remaining}$ remains constant. In this case, the link cost increases when $(\Delta dh+1)$ increases. On the other hand, suppose $(\Delta dh + 1)$ remains constant. In this case, the link cost increases as $e_{j,remaining}$ decreases. The weight factor δ adjusts the priority. A large δ gives more weight to the node energy than to the hop distance.

Link quality is determined from received signal strength value and signal to noise ratio value. Signal to Noise Ratio influences the bit error rate that a packet is successfully transferred. Here we include the packet dropping ratio for determining the path quality. It is defined as the number of packets dropped to the total number of packets received in the particular link. Bit Error Rate is inversely proportional to the SNR. The SNR is derived as

$$SNR = \frac{S_R}{\sum_{i \neq R} P_u + N_K} \quad (2)$$

In case if the disjoint network occurs, the load balancing is required. Here, there are M disjoint paths between a source node S and a sink node D. The requested data rate to be arrived at the sink node D via all these multipaths is R bits/sec. Let f_j be the data rate allocated to path j. For a path j, the product of the path cost p_j and the data rate allocated f_j gives the path cost rate w_j.

$$\Phi(f) = \frac{\left(\sum_{j=1}^{M} f_j p_j \right)^2}{M \sum_{1}^{N} (f_j p_j)^2} \quad (3)$$

where the vector denotes the traffic rates allocated to all available routes and f_j is the traffic flow allocated to path j. The idle period of the wireless channel is a key parameter to determine the average bandwidth which is determined by the traffic travelling along the mobile nodes as well as their neighbor nodes. During that period the mobile nodes can successfully transmit data packets.

$$Avg_{bw} = Max_{bw} \otimes \left(\frac{Idle_t}{Initial_t} \right) \otimes L_q \quad (4)$$

Where L_q is the link quality.

$$E_{j,remaining} = E_{j,INIT} - E_j \quad (6)$$

IV. PERFORMANCE ANALYSIS

We use Network Simulator (NS 2.34) to simulate our proposed REMRA algorithm. Network Simulator-2(NS2.34) is used in this work for simulation.NS2 is one of the best simulation tools available for Wireless sensor Networks. We can easily implement the designed protocols either by using the oTCL (Tool command Language) coding or by writing the C++ Program. In either way, the tool helps to prove our theory analytically.

In our simulation, 200 mobile nodes move in a 1200 meter x 1200 meter square region for 60 seconds simulation time. All nodes have the same transmission range of 250 meters. Our simulation settings and parameters are summarized in table 2.

A. Performance Metrics

We evaluate mainly the performance according to the following metrics.

End-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Packet Delivery Ratio: It is defined as the ratio of packet received with respect to the packet sent.

Throughput: It is defined as the number of packets received at a particular point of time

The simulation results are presented in the next part. We compare our proposed algorithm REMRA with NMRA and SBYaoGG [15], AFTMR[16] in presence of energy consumption.

Table2. Simulation settings and parameters of proposed algorithm.

No. of Nodes	300
Area Size	1300 X 1300
Mac	802.11
Radio Range	500m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Transmitter Amplifier	150 pJ/bit/m^2
Package rate	5 pkt/s
Protocol	AODV

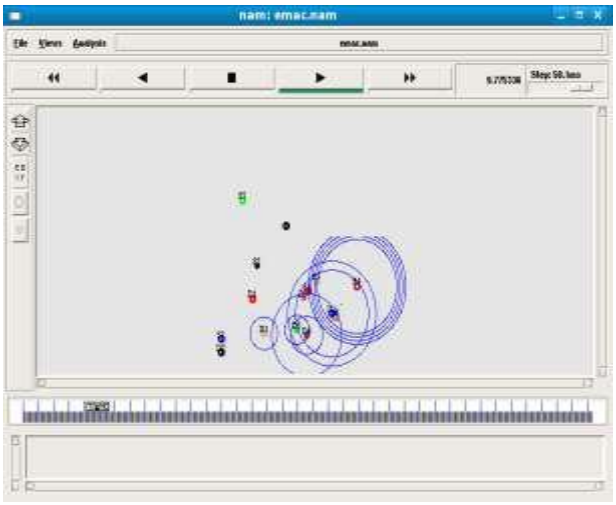

Figure 3. Topology of the proposed scheme

Figure 3 shows that the proposed scheme topology for ensuring the multipath routing. Source node sends the packet to destination node via intermediate nodes. In case if the node failure occurs, the node choose the alternative path to reach correct delivery of packets.

Figure 4 shows the results of average residual energy for varying the time from 10 to 50 ms. From the results, we can see that scheme REMRA has minimal energy consumption than the NMRA, AFTMR and SBYaoGG scheme.

Figure 5 presents the delivery ratio comparison for REMRA, NMRA, SBYaoGG. It is clearly seen that number of epochs consumed by REMRA is high compared to SBYaoGG, AFTMR and NMRA.

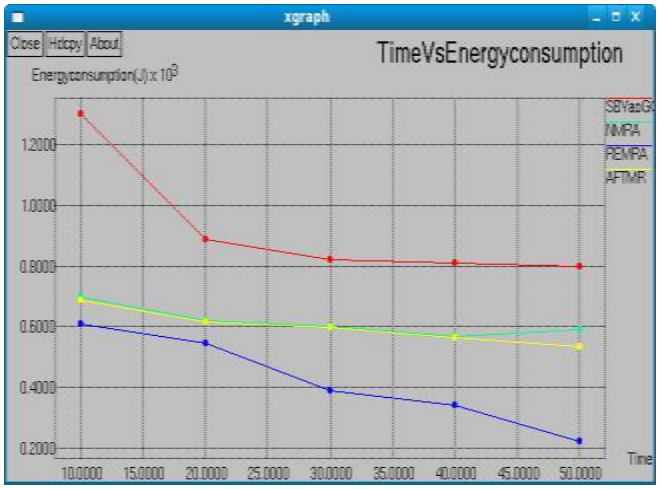

Figure 4. Time Vs Energy consumption

Figure 5. No.of Nodes Vs Packet Delivery Ratio

V. CONCLUSION

In WSNs, the best secure and energy efficient route is being determined by choosing efficient strategy to forward the data to the base station. Due to that, the node consumes more energy unnecessarily. In this paper, we have developed a Residual Energy based Multipath Routing Approach (REMRA) which attains correct balance between energy consumption and authentication to the sensor nodes. In the first phase of the scheme, concept of proposed multipath routing is explained. In second phase, the path stability is determined to ensure the network connectivity. In third phase, residual energy consumption and secure routing is established. The proposed scheme uses following factors called path stability, residual energy and authenticity to favor packet forwarding by maintaining high residual energy consumption and secure routing for each sensor node. We have demonstrated the residual energy determination of each sensor node. By simulation results we have shown that the REMRA achieves good throughput, high network lifetime, high residual energy while attaining low delay than the proposed scheme NMRA and existing schemes SBYaoGG, AFTMR while varying the number of nodes, time, node throughput and mobility.

Reference

[1]Shuang Li, Raghu Kisore Neelisetti, Cong Liu and Alvin Lim, "Efficient Multi-path protocol for Wireless Sensor Networks", International Journal of Wireless & Mobile Networks, Vol.2, No.1, 2010, pp.110-130.

[2]Hamid reza Hassaniasl, Amir masoud Rahmani, Mashaallah Abbasi Dezfuli and Arash Nasiri Eghbali, "A Novel Score-Aware Routing Algorithm in Wireless Sensor Networks",International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (5), pp.397 – 404.

[3]Yuxin Mao and Guiyi Wei, "A Feedback-Based Secure Path Approach for Wireless Sensor Network Data Collection", Sensors, 2010, Vol.10, pp.9529-9540

[4]S. Saqaeeyan and M. Roshanzadeh, "Improved Multi-Path and Multi-Speed Routing Protocol in Wireless Sensor Networks", International Journal of Computer Network and Information Security, 2012, Vol.2, pp.8-14.

[5]Yuxin Mao and Guiyi Wei, "A Feedback-Based Secure Path Approach for Wireless Sensor Network Data Collection", Sensors, 2010, Vol.10, pp.9529-9540

[6]S. Saqaeeyan and M. Roshanzadeh, "Improved Multi-Path and Multi-Speed Routing Protocol in Wireless Sensor Networks", International Journal of Computer Network and Information Security, 2012, Vol.2, pp.8-14.

[7]M.Riyaz Pasha and B.V.Ramana Raju, "A Self-Optimized Multipath Routing Protocol forWireless Sensor Networks", International Journal of Advacnes in Computer Networks and its Security, pp.203-207.

[8]S. Ganesh and R. Amutha, "Efficient and Secure Routing Protocol forWireless Sensor Networks through Optimal Power Control and Optimal Handoff-Based Recovery Mechanism", Journal of Computer Networks and Communications, Article ID 971685, pp.1-8.

[9]Reza Azarderskhsh and Arash Reyhani-Masoleh, "Secure Clustering and Symmetric Key Establishment in Heterogeneous Wireless Sensor Networks", EURASIP Journal on Wireless Communications and Networking, Volume 2011, Article ID 893592, pp.1-8.(0975 – 8887) Volume 21– No.5, May 2011, pp.20-26.

[10]S. Saqaeeyan and M. Roshanzadeh, " Improved Energy Aware and Two Hop Multipath RoutingProtocolinWirelessSensorNetworks",International Journal of Computer Network and Information Security, 2012, Vol.5, pp.22-28.

[11]Jayashree Agarkhed, G. S. Biradar and V. D. Mytri, "Energy Efficient QoS Routing in Multi-Sink Wireless Multimedia Sensor Networks", International Journal of Computer Science and Network Security, VOL.12 No.5, May 2012, pp.25-31.

[12]Mary Cherian, T. R. Gopalakrishnan Nair,"Multipath Routing With Novel Packet Scheduling Approach In Wireless Sensor Networks",International Journal of Computer Theory and Engineering, Vol. 3, No. 5, October 2011, pp.666-670.

[13]Venkata Sumanth Mareedu, Sudheesha Cheepi and Venkata Durga Kiran Kasula, "Data Transferring Mechanisms for Multipath Routing Using Concentrated Dissimilate Algorithm in Wireless in Wireless Networks", International Journal of Computer Trends and Technology-Vol.3, Issue1-2012, pp.53-57.

[14]S.Pratheema, K.G.Srinivasagan and J.Naskath, "Minimizing End-to-End Delay using Multipath Routing in Wireless Sensor Networks",International Journal of Computer Applications

[15]Tapiwa M. Chiwewe, and Gerhard P. Hancke, "A Distributed Topology Control Technique for Low Interference and Energy Efficiency in Wireless Sensor Networks", IEEE Transactions on Industrial Informatics, Vol. 8, No. 1, February 2012, pp.11-19.

[16]K. Vanaja and R. Umarani, "An Adaptive Fault Tolerant Multipath Routing (AFTMR) Protocol for Wireless Ad Hoc Networks", European Journal of Scientific Research, ISSN 1450-216X Vol.79 No.2 2012, pp.180-190.

Author Profile

Harikrishnan G, received his M.Tech degree in Remote Sensing And Wireless Sensor Networks from Amrita Vishwa Vidyapeetham , Ettimadai ,Coimbatore. He received his B.E in Electronics and Communication Engineering from Tamilnadu College of Engineering, Anna University Chennai. His research areas include Digital Image Processing, Software Defined Radio, Wireless sensor Networks, CUDA, Deep space and Hyper spectral Image processing. Currently he is working as Assistant Professor in Electronics and Communication Engineering at Nirmala College of Engineering, Chalakudy ,Calicut University, Kerala.