ISSN 2047-3338

An Efficient Reactive Routing Security Scheme Based on RSA Algorithm for Preventing False Data Injection Attack in WSN

Veena Janardhanan[1], Arun Jose[2], Parameshachari B. D.[3], Muruganantham C.[4] and H. S. DivakaraMurthy[5]
[1,2,3,4,5]Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India
[1]veenajanardhanan86@gmail.com, [3]parameshbkit@gmail.com

***Abstract*– Wireless sensor networks are vulnerable to various attacks. Injecting false data attack is one of the serious threats to wireless sensor network. In this attack adversary reports bogus information to the sink which causes error decision at upper level and energy waste in en-route nodes. Several authentication techniques using enroute filtering and cryptographic techniques are used for preventing such attacks. This paper focuses on the design of RSA based security scheme with on demand routing. On- demand routing protocol is used in this scheme to lower the energy consumption. This work evaluates and compares the performance of the network system using RSA algorithm and authentication algorithm. Study and implementation of these security schemes are been carried out using network simulator (ns2) and metrics such as Packet Delivery Ratio, Energy, Throughput. Results are presented as a function of these metrics and the graphs generated show that RSA based security scheme with on-demand routing performs better than the security schemes using authentication algorithms.**

***Index Terms*– False Data Injection, RSA Algorithm, On-Demand Routing, Performance Evaluation and Wireless Sensor Network**

I. INTRODUCTION

WIRELESS Sensor Networks have emerged as an important new area in wireless technology. Wireless sensor networks can be deployed in large scale for performing environmental and habitat monitoring, surveillance and tracking purposes for military. Security will be one of the main concerned when they will be deployed in large scale. Deployment of wireless sensor networks is usually done at adverse or unaccompanied environments. Therefore, the networks are prone to be attacked by adversaries who intend to disrupt the functioning of the system by compromising the sensor nodes and injecting false data into the network.

For an injecting false data attack, an adversary first compromises several sensor nodes, accesses all keying materials stored in the compromised nodes, and then controls these compromised nodes to inject bogus information and send the false data to the sink to cause upper-level error decision, as well as energy wasted in en-route nodes. For instance, an adversary could fabricate a wildfire event or report wrong wildfire location information to the sink, and then expensive resources will be wasted by sending rescue workers to a nonexistent or wrong wildfire location. At the same time, if all false data are flooding into the sink simultaneously huge energy will be wasted in the en-route nodes as a result; the whole network could be paralyzed quickly. So it is important to shield the sensor network from false data injection attack.

Authentication schemes based on en-route filtering is one of the effective ways to defeat false data injection attacks. The ultimate objective of en-route filtering is to improve the resilience against node compromisations. In en-route filtering not only the destination node but also the intermediate nodes can check the authenticity of the message in order to reduce the number of hops the false message travels and thereby conserves energy. In the en-route filtering phase, the en-route node receives a report from the source node or the lower associated enroute node and check the integrity of the received report by means of the MAC enclosed in the report. If the verification succeeds then forward the report otherwise drop the report.

The paper is organized as follows: Section 2 discusses the brief overview of related work. Section 3 describes the proposed method. Section 4 shows experimental results. Finally in Section 5 the conclusion is described.

II. RELATED WORKS

Lot of research works are going on in the field wireless sensor network security. Each day a new idea on this subject is being put forward. The unattended operation makes it easy to compromise the sensor node and to release the information to the adversary .Adversary can launch internal attack that cannot be solved by cryptographic technique .Such internal attacks can be solved by en-route filtering schemes. En-route filtering schemes are useful in mitigating false data injection attack and path based DOS attack because the falsified messages will be filtered out as soon as possible. For the successful outcome of this project here referred some different sides of the enrooting filtering mechanism and its drawbacks.

One of the en-route filtering scheme is Statistical en-route filtering scheme [5]. It addresses the fabricated report injection attacks in the presence of compromised nodes and introduces an en-route filtering framework. In SEF, there is a global key pool, which is divided into n non-overlapping partitions. Before deployment, each node stores a small number of authentication keys randomly selected from one partition of globe key pool. Nodes with keys from same partition are considered as the same group. In this way, all nodes are divided into n groups via non-overlapping key partitions. The SEF scheme adopts T-authentication, that is, the legitimate report must carry T MACs generated by T nodes from different groups. Each of these T nodes generates MAC with one of authentication keys it stored.. Each event detecting sensor endorses the report by producing a keyed MAC using one of its stored keys. A report with insufficient number of MACs will not be forwarded. When the sink receives event reports, it can verify all the MACs carried in the report because it has complete knowledge of the global key pool. False reports with incorrect MACs that pass through en-route filtering will then be detected. The SEF mechanism detects and drops bogus reports from compromised nodes. The verification of MACs is done probabilistically. SEF cannot detect which nodes are compromised because reports are filtered en-route probabilistically, but it can prevent the false data injection attack with 80 - 90 percent probability within 10 hops. In SEF if anode is compromised the attacker can obtain the keys for number of compromised nodes since more than one node store keys from common key pool.

Another method is an interleaved hop-by-hop authentication (IHA) scheme [6]. In this scheme, the base station periodically initiates an association process enabling each node to establish pair wise keys with other nodes that are n hops away, which is a security threshold. All nodes are detecting nodes and forwarding nodes, generating reports about events, forwarding them and verifying report correctness. At least t+1 node must agree on a report for it to be considered valid. The drawback of IHA is, it requires the existence of a fixed path for transmitting control messages between the base station and every cluster head. Other problem in IHA is every en-route node must exchange its associated key with lower and upper associated node. The high communication overhead incurred by the association process makes IHA unsuitable for the networks whose topologies change frequently.

Yang et al. [2] proposed a Location-Based Resilient Secrecy. Location-based resilient security (LBRS) scheme is another security scheme .LBRS has a major improvement over SEF, and mitigates T-threshold limitation problem in SEF by location-ware authentication key. In LBRS, a sensing field is divided into square cells, and each cell is associated with some cell keys that are determined based on the cell's location. Each node stores two types of cell keys. One type contains the keys bounded to their sensing cells to authenticate the reports from those cells. The other type contains the keys of some randomly chosen remote cells, which are very likely to forward their reports through the node's residing cell. In LBRS, a forwarding node verifies the received reports and filters out false ones in the same way as SEF. LBRS suffers a severe drawback. It assumes that all the nodes can determine their locations and generate location-based keys in a short secure time slot. However, to the best of our knowledge, most of the practical sensor localization approaches cannot be finished in such a short time slot, and even the localization process itself is vulnerable to various attacks. In addition LBRS cannot work effectively in the networks with mobile sink and various routing protocols.

Ren et al. [3] proposed more efficient location-aware end-to-end data security design (LEDS) which provides end-to-end security for false data filtering. Since LEDS is a symmetric key based solution, the location-aware key management is required to achieve en-routing filtering. Zhang et al. [4] provides a location-based keys system to address this problem. This system binds individual private keys of individual nodes to both their IDs and geographic locations and a suite of location-based compromise-tolerant security.

BECAN [1] achieves high filtering and reliability when compared with other en-route filtering mechanisms. In BECAN each node requires fixed (k) number of neighbors for co-operative neighbor router (CNR) based authentication. BECAN filter injected false data through cooperative authentication of the event report by k neighboring nodes of the source node. BECAN distributes the authentication of en-routing to all sensor nodes along the routing path to avoid complexity. This scheme adopts bit- compressed authentication technique to save bandwidth. This technique is suitable to handle compromise and filter injected false data in wireless sensor networks.

A) Review of BECAN Scheme

Network model of this scheme consists of a sink and a large number of sensor nodes randomly deployed at a certain interest region. Sink is a data collection unit.Since a wireless sensor network is unattended; a malicious adversary may readily launch some security attacks to degrade the network functionalities. In addition, due to the low cost constraints, sensor nodes are not equipped with expensive tamper-proof device and could be easily compromised in such an unprotected wireless sensor network. Therefore, in security model, assume an adversary A can compromise a fraction of sensor nodes and obtain their stored keying materials. Then, after being controlled and reprogrammed by the adversary A, these compromised sensor nodes can collude to launch some injected false data attacks. Mainly it consists of MAC generation and MAC verification. When a sensor node generates a report m after being triggered by a special event, e.g., a temperature change or in response to a query from the sink, it will send the report to the sink via an established routing. Assume that, the sensor (source) node has sensed some data m and is ready to report m to the sink via the routing path. The source node gains the current timestamp T, chooses k neighboring nodes and sends the event (m,T) and routing to neighboring nodes. With (m,T,RN0)as input, each sensor node generate a row authentication vector and reports row authentication vectors to the source node. After the source node aggregates all row vectors it formats the authentication information MAC and reports (m,T, MAC) as well as to the sink along the routing .

To filter the false data injected by compromised sensor nodes, the BECAN adopts cooperative neighbor × router (CNR)-based filtering mechanism. For the MAC generation MAC algorithm used is MD5 algorithm. In MAC verification every forwarding node verifies the MAC computed by its lower association node, and then removes that MAC from the received report. If the verification succeeds, it then computes and attaches a new MAC based on its pair wise key shared with its upper associated node. Finally, it forwards the report to the next node. That is when each sensor node along the routing (m,T, MAC) from its upstream node, it checks the integrity of the message m and the timestamp T. If the timestamp T is out of date, the message (m,T, MAC) will be discarded.BECAN scheme can detects gang injection false data attack from mobile compromised sensor nodes using Ad hoc on-demand distance vector (AODV) routing protocol.MAC algorithm used in this scheme provides only an authentication to the system and one of the main disadvantage of MAC algorithm is cryptographic weakness.To make the system more secured and to eliminate cryptographic weakness this system can be modified using RSA algorithm.

III. PROPOSED SCHEME

A security scheme is designed using RSA algorithm to avoid cryptographic weakness.RSA algorithm is used in this modification and it is used for generating and establishing pair wise key Routing protocol used is dynamic source routing protocol. In this scheme network model consists of large number of sensor nodes is initially designed. After the design of network model keys for each sensor nodes are generated using RSA algorithm. Both private and public key are generated. After key generation each of the nodes ensures that whether neighboring nodes are secured or not.

Next step is the routing implementation using routing protocol. Reactive routing protocol known as on-demand routing protocol is used in this security scheme. In this routing paths are searched only when needed. They use a discovery procedure to terminate either when a route has been found or when no route is available after examination for all route combinations. Less control overhead, better scalability, and longer battery power are advantages of reactive routing over proactive routing protocols.

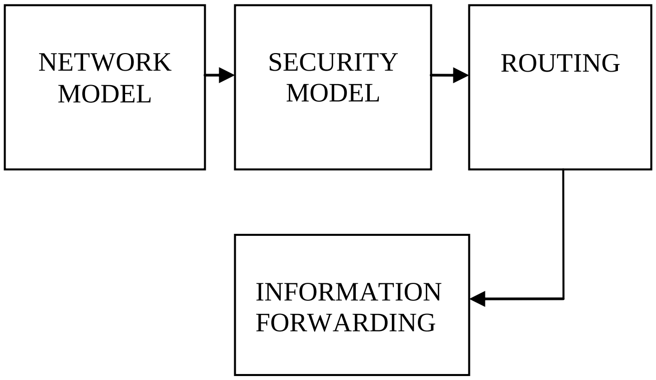

Figure 1: Block diagram of modified security scheme

In this scheme when an event is triggered source node senses the event and information is forwarded to the destination through routing nodes based on routing algorithm. After the key generation and route maintenance information to be forwarded is encrypted using public key and at destination it is decrypted using private key.

A) Network Model

Network model defines how the network is formed. In this paper assume a wireless sensor network having 100 sensor nodes.Large number of sensor nodes are randomly deployed at a certain interest region (CIR) with the area S in wireless sensor network. Network model consists of sink which is a trustable and powerful data collection device. Sink has sufficient computation and storage capabilities and is responsible for initializing the sensor nodes and collecting the data sensed by these nodes. For differentiation purpose, assume each sensor node has a unique nonzero identifier.Each sensor node is equipped with omnidirectional antennas.

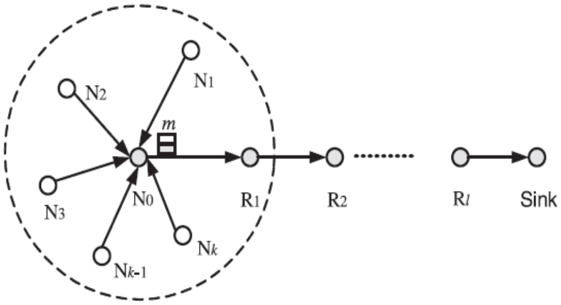

Figure 2: Network model

The closer sensor node to the sink can have direct contact with sink. The farther sensor node from the transmission range of the sink has to establish the route to communicate with the sink. The communication is bidirectional i.e. two sensor nodes within their wireless transmission range (R) may communicate with each other.

B) Security Model

Keys for each sensor nodes are generated using RSA algorithm.RSA algorithm generates both private and public key for each node. After key generation each of the nodes ensures that whether neighboring nodes are secured or not.

RSA Algorithm:

STEP1: Choose 2 large prime numbers p &q at random

STEP2: Obtain n=p*q

STEP3: Euler quotient function of n,z=(p-1)(q-1)

STEP4: Choose Public key,e in such a way that it should be less than n such that e&z are relatively prime

STEP5: Choose Private key, d such that when ed is divided by z remainder is 1(d=e inverse mod z)

C) Routing

Routing algorithm helps to find a path from a designated source node, usually the current position, to a designated destination**.** In this system we are using Dynamic source routing algorithm. Dynamic Source Routing (DSR) protocol is a reactive unicast routing protocol that uses source routing algorithm. In DSR, each data packet contains whole routing information to reach its destination and caching technology is used by each node to maintain learnt route information. DSR uses route discovery phase and route maintenance phase for sending and receiving information or packets between nodes. When a link disconnection is been detected by the data link layer, a ROUTE_ERROR packet is sent backward to the source and the source node initiates a route discovery operation. When the ROUTE_ERROR packet is transmitted to the source, the broken link route is removed from the route caches of the immediate nodes. It adjusts to changing network circumstances by analyzing incoming routing update message. If the message indicates that a network change has occurred, routing software recalculates routes, sends out new routing update messages.

D) Information Forwarding

When an event is triggered information is forwarded from source node to destination through routing path using routing algorithm. Before forwarding information to the next node message is encrypted using public key and at destination it is decrypted using private key.

E) Implementation and Methodology

Software Specifications:

1.	OS	: Linux (VMware)
2.	Simulator	: NS2
3.	Language	: Tcl/Tk
4.	Graph	: GNU plot
5.	Protocol Design	: CC

Hardware Specifications:

1.	Processor Type	: Pentium IV
2.	Processor Speed	: 2.7GHz
3.	RAM	: 1GB

IV. RESULTS AND DISCUSSION

A) Simulation Setup

We have used NS2 for the simulation of the proposed security scheme. Network Simulator 2 (NS2) used is a discrete event driven simulator developed by UC Berkeley. The parameters used and their values are shown in the Table 1.

Table 1: Simulation Parameters

Parameters	Value
Routing protocols	DSR,AODV
MAC	802.11
Terrain Size	2500m*1000m
Nodes	100
Traffic	Tcl

The following metrics were used to evaluate the performance of routing protocols discussed above and Figure 3 to Figure 5 show the graph generated. First is energy saving. It shows the total energy consumption for the security scheme.

Total energy consumed for all the protocols is directly proportional to the number of transmissions, which is the sum of the number of data packets sent and the number of control packets sent per node.Next is Packet Delivery Ratio (PDR).This is the ratio of packets delivered to the destination to the packet generated by the sources. PDR = (Pd/Ps)*100 Where Pd is total packet delivered to the destination and Ps is total packet sent. Third one is throughput which is defined as the average rate of successful message delivery over a communication channel or sum of the data rates that are delivered to all nodes in a network. As there is heavy packet loss with the presence of malicious activity, the throughput of the network is declined.

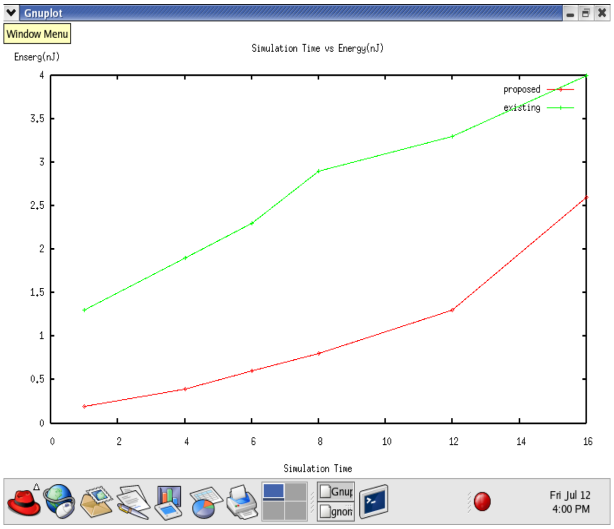

Figure 3: Energy vs. Simulation Time

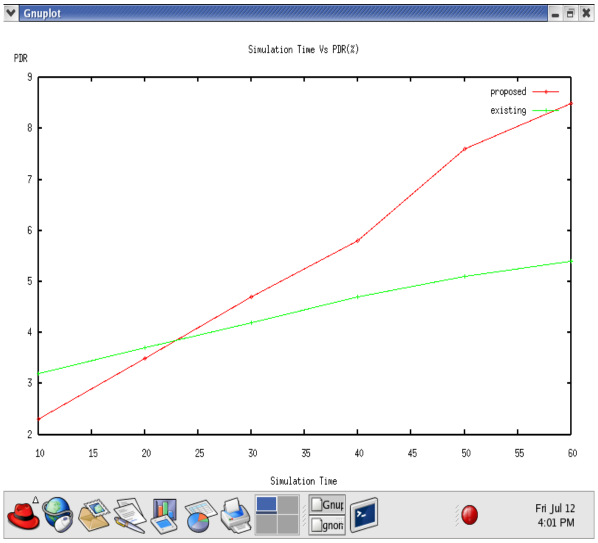

Figure 4: PDR vs. Simulation Time

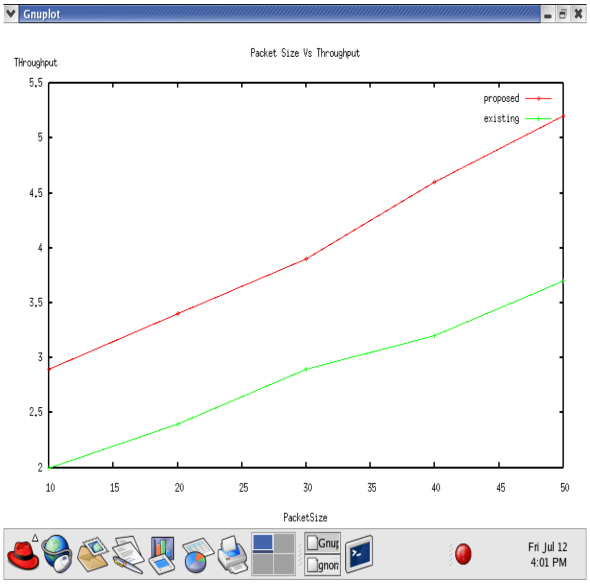

Figure 5: Throughput vs. Simulation Time

The result of this work is based on the performance of the two security schemes i.e., BECAN authentication scheme and RSA algorithm based security scheme with on-demand routing used during the simulation. The same number of simulation parameters were used under the same simulation environment and a number of random traffic were generated. The Figure 3 to Figure 5 display the result and highlight the relative performance of them RSA algorithm based security scheme with on-demand routing. In energy consumption RSA based security scheme performs better irrespective of simulation time as shown in Figure 3. Packet delivery ratio in RSA algorithm based security scheme is much in Figure 4 due to the absence of packet loss. In Figure 5, RSA algorithm based security scheme has higher throughput than BECAN scheme based on MAC algorithm. Graphs generated shows that RSA based security scheme performs better than MAC based BECAN with AODV.

V. CONCLUSION

This work determines the performance of RSA based security scheme with on-demand routing for preventing false data injection attack in wireless sensor network using ns-2 simulations. RSA algorithm used in the modified scheme provides greater security to the system than MAC algorithm in the BECAN scheme.MAC algorithm provides only an authentication to the system but RSA algorithm makes the system more secured by public key cryptographic technique. Both AODV and DSR routing algorithms in these two security schemes use the reactive on-demand routing strategy. While AODV uses routing tables, each per destination and sequence number to avoid loops and to find fresh route, DSR uses source routing and route caches and do not rely on any periodic or timing activities. But DSR maintains multiple routes for destination aggressive caching help DSR to keep its routing load down. Performance evaluations of both systems are in terms of energy, packet delivery ratio, and throughput. In the performance evaluation RSA based security system has higher values of energy, packet delivery ratio and throughput. It is observed from the simulation that security scheme using RSA algorithm performs better than MAC algorithm based BECAN authentication scheme with AODV routing.

ACKNOWLEDGEMENT

The work described in this paper is supported by Adv. Dr. P. Krishnadas, Managing Trustee and Dr. P. Krishnakumar, CEO & Secretary, Nehru Group of Institutions, Tamil Nadu, Kerala-India. Authors are grateful to Prof. Dr. P. N. Ramachandran, Principal and Dr. N. K. Shakthivel, Vice Principal, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India, for providing us the opportunity to undertake this project.

REFERENCES

[1]. Rongxing Lu, Student Member, IEEE, Xiaodong Lin, Member, “BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks” IEEE transactions on parallel and distributed systems, vol. 23, no. 1, january 2012

[2]. H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, “Toward Resilient Security in Wireless Sensor Networks,” Proc. Sixth ACM Int’l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc ’05), pp. 34-45, 2005.

[3]. K. Ren, W. Lou, and Y. Zhang, “LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks,” Proc.IEEE INFOCOM ’06, Apr. 2006.

[4]. Y. Zhang, W. Liu, W. Lou, and Y. Fang,“Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks,” IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 247-260, Feb. 2006.

[5]. F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks,” Proc. IEEE INFOCOM ’04, Mar. 2004. 43-856, 2010

[6]. S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks,” Proc. IEEE Symp. Security and Privacy, 2004.

Veena Janardhanan studying M. Tech degree course in applied electronics and communication systems at Nehru College of engineering and research centre thrissur, under University of Calicut.

Arun Jose working as a Assistant Professor in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre, Kerala, India. He worked as Systems Engineer with ABB, UK for Four years. He obtained his B. Tech in Electronics and Communication Engineering from Vellore institute of Technology, Vellore, India and M S from Liverpool John Moores University, UK. He is member of IET. His area of interest is wireless communication, Mobile Computing and VLSI.

Parameshachari B. D. working as an Associate Professor in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India, affiliated to University of Calicut. Worked as a Senior Lecturer and inchage HOD in the Department of Electronics and Communication Engineering at JSS Academy of Technical Education, Mauritius. He worked at JSSATE, Mauritius for Three years and also worked as a Lecturer at Kalpatharu Institute of Technology, Tiptur for Seven years. He obtained his B.E in Electronics and Communication Engineering from Kalpatharu Institute of Technology, Tiptur and M. Tech in Digital communication Engineering from B M S college of Engineering, Bangalore, affiliated to Visveswaraiah Technological University, Belgaum. He is pursuing his Ph.D in Electronics and Communication Engineering at Jain University, Bangalore, Karnataka, India under the guidance of Dr. K M Sunjiv Soyjaudah, Professor, University of Mauritius, Reduit, Republic of Mauritius and Co-guidance of Dr. Sumithra Devi K A, Professor and Director, Department of MCA, R V College of Engineering, Bangalore. Parameshachari area of interest and research include image processing, cryptography and Communication. He has published several Research papers in international Journals/conferences. He is a Member of ISTE, IETE, IACSIT, IAEST, IAENG and AIRCC.

Muruganantham. C. working as a Assistant Professor in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre,kerala,India. He obtained B.E in ECE from Madurai Kamaraj University,Tamilnadu and M.E in Applied Electronics from Anna University,Tamilnadu. Worked as Assistant Professor-II in SEEE of SASTRA University. Worked as Lecturer in Electrical & Computer Engg Department of Ethiopian Universities. Published papers in national/international conferences. He is member of ISTE. His areas of interest are High Speed VLSI Networks, Signal Processing.

Divakara Murthy H. S. has multi faceted experience in Research, Industry and Academic fields, He is working as a Dean and HOD in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India, affiliated to University of Calicut and also served as a Principal at JSS Academy of Technical Education, Mauritius for two years. Involved in Administrative & Academic activities in development of infrastructure facilities marketing, mounting new courses and strategic planning. He worked at RGV telecom Ltd Bangalore as Deputy Vice president,for providing optical communication for Indian Railways for nealy two years and also worked nearly 27 years in Telecom in Industry at senior level in various capacities in Telecom Projects and Planning, Production and Marketing. During my intial career involved in Design and development of Instrumentation at NAL Bangalore. He obtained his B.E in Electronics and Communication Engineering from Siddaganga Institute of Technology, Tumkur from University of Mysore and MSc (Engg.) in communication system from PSG Institute of technology, Coimbatore , from University of Madras. Divakara Murthy area of interest and research include Micro and Pico Satellite communication, Optical Communication and Wireless communication, GSM and WiMAX technology. He is a Member of ISTE, IETE.