Reliable Security Wireless Sensor Network Using SCTP

R.Kanthavel [£] , L.Ganesan [#] and R.Dhaya [µ],

Govt College of Engg,Tirunelveli A.C. Tech, National Engg College,Tamilnadu,India

Summary

Any network is said to be an intelligent one, only when the nodes of the network can have the ability to contact the other nodes without wire and being away from difficulty by means of congestion, late response and late acknowledgement. So here we propose to implement a wireless sensor network for mobile nodes and Bluetooth for reducing the above said difficulties by the way of applying parent search routing and using SCTP in the tree topology network, where hierarchical Connection of nodes involve. We simulate our proposed network to get animated output for the inquiry time and transmission time.

Key words: *Parent search routing, Tree topology, SCTP, Intelligent network*

1. Introduction

A sensor network is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it. The positions of sensor nodes need not to be engineered or predetermined which allows random deployment in accessible terrains or disaster relief operation. Whenever they are set up, cables must link the sensor nodes to a system and if cable links to sensor nodes, it will not only cost a great deal but also hard to maintain.

Moreover it is hard to change a position of a sensor node, and if there is an accident such as a disaster that destroys the wired network and hence wireless sensor network is preferable. Wireless sensor networks consist of a large number of densely deployed sensor nodes. These nodes incorporate wireless transceivers so that communication and networking are enabled. Additionally, the network possesses self-organizing capability so that little or no network setup is required.

In this paper we instead concentrate on Mobile technology and Movable nodes for security system and the protocol used is SCTP. Our security model has been explained in the below

1.1 System Overview

We first introduce an overall working flow of the system and then explain the initialization procedure for network configuration and routing. Finally, we introduce the operation of each node in the system in more detail.

The purpose of the proposed system is for detecting an invasion in a building or any environment that needs security service, and the network consists of lots of sensor and relay nodes and a control node. Figure 1 illustrates the communication environment of the system.

The proposed network consists of

- Sensor nodes
- Relay nodes
- Control node.

All nodes communicate with each other with the wireless module (Bluetooth module, Mobile module (separately configured)).Sensor and relay nodes detect certain events (e.g. someone enters the security area without permission) and report the events to the control node. Then, the control node reports the information received from the sensor or relay nodes to the local security control system and replies to the corresponding node with an ACK message. If sensor nodes are not able to directly reach the control node, the relay nodes placed between them can relay the message from the sensor node to the control node. All nodes transmit and receive packets via a wireless module (Bluetooth, Mobile) that is embedded in them. In this paper, we introduce the implementation issues related to the proposed network.

Sensor nodes are placed in each room in the building and logically connected to the control node, which is located at a certain place in the building and can be reached via relay nodes.

Sensor and relay nodes detect certain events and report it to the control node. Then the control node reports the event received from the sensor or relay node to the local security control system and replies to the corresponding node with an *ACK* packet. The node which had sent an event packet must receive an *ACK*

Manuscript received May 5, 2007
Manuscript revised May 20, 2007

packet from the control node to verify that the event packet was delivered to the control node. If sensor nodes are not able to directly reach the control node, the relay nodes placed between them relay the message from the sensor node to the control node. That is, if a sensor node is not able to inquire the control node (i.e., the control node is located outside the range of a sensor node), relay nodes placed between them form a route from the sensor node to the control node. All nodes transmit and receive packets via modules embedded in them.

When a phenomenon is detected by a sensor or relay node, such an event is translated to a predefined value corresponding to that event, and then it is transmitted in the form of an event packet to the control node via the radio link. In this paper, we assume that sensor and relay nodes have on-off switches to emulate certain events, e.g., the motion detectors in those nodes detect a movement, for convenience.

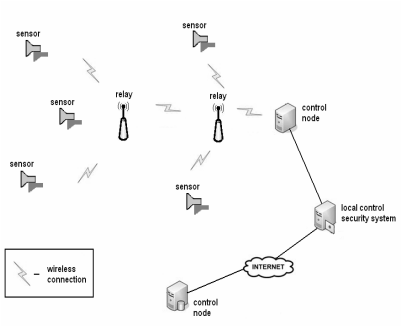

Figure 1: System overview

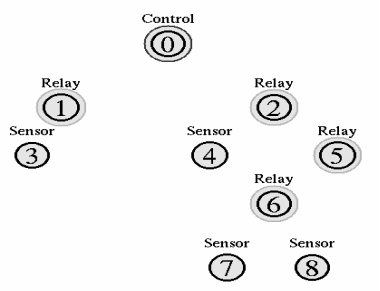

Figure 2: System Configuration

Our proposed system is compatible with the deployment of Bluetooth and Mobile nodes and we have created node movement which will further enhance our system configuration

2. Existing Problems

We have proposed wireless sensor network with the deployment of mobile and we confronted some problem while implementation to overcome the problem of coverage area of using Blue tooth technology in the existing.

2.1 Range limitation Bluetooth

Scatter net implementation of Bluetooth even though wise selection for security system range of its communication has created concern over its placement. Sensor and relay must be placed within its communication range. This put restriction with system configuration.

2.2 Problem confronted with TCP protocol:

- Multimedia communities find the congestion control mechanisms TCP employs are too restrictive.
- Wireless and mobile users also find that TCP reacts badly to losses and delay variations due to wireless links or handovers.
- The signaling community has found that TCP service is too restrictive for their needs.
- Without modification, it was clear that TCP/IP could not allow a user to roam between different networks while maintaining connectivity to the Internet.

2.3 Security problem with ADHOC network

Because of the vulnerabilities in the physical security ad hoc routing protocols are exposed to many kinds of attack. Maintaining link layer security is in practice harder with ad hoc networks than with fixed networks. Sufficient routing protocols security is desirable. Sufficient within this context covers prohibiting disruption or modification of protocol operation.

2.4 Problem with fixed wireless network

Wireless sensor network takes some advantage over wired network. But the problem is not completely over. Depth of network can be increased by placing more sensor nodes. But this placement requires additional relays which may increase the system installation.

3. Our Proposed Solution

In our paper we have simulated wireless sensor network using both Mobile and Bluetooth nodes.

3.1 Deployment of Mobile nodes

Range limitation of Bluetooth models can be put an end by the deployment of Mobile nodes where range of communication is more.

3.2 Deployment SCTP protocol

Our project focuses on the effect of using SCTP instead of TCP over a Mobile network. It introduces some unusual configurations, which suggest that SCTP is worthy of further research in the mobile/wireless domain.

3.3 Deployment of Tree topology and parent search algorithm

Our system configuration is simple not prone to security preach because the sensor node of interest will only communicate its nearby parent according to our proposed parent search algorithm. We have formulated isolated point to point communication, which further develops itself and forms tree configuration. Our routing procedure does not follow adhoc routing and so path can be predicted easily. We can also predict if any intrusion occurs with relay nodes. In this way, we have overcome security problem of adhoc network.
The tree topology has a advantage of finding a multi-hop route to the control node or a specific node easily, to maintain network structure, control medium access and transmission timing.

3.4 Node movement

In the previous section we have mentioned problem with the fixed wireless network. Our solution postulates that depth of the tree can be increased without modifying number of relay nodes such that existing relay nodes will take the responsibility over newly created nodes.

3.5 Parent search routing algorithm

Routing of packets is a very simple matter in our proposed system, since data packets sent by sensor or relay nodes are always destined for the control node and a free topology is adopted for the network configuration. Our routing algorithm has been shown in the flowchart. When one object introduces the jurisdiction of one sensor node, it detects the event, and starts to send the information through the near by node to control hub.
Let us see how our algorithm manipulates sensor node and router nodes to perform inquiry procedures.

3.5.1 Inquiry Procedure

Our proposed inquiry procedure first starts to search its neighbors and gets their logical addresses. Analyze neighbor's logical address and finds its parent and other neighbors. Then creates one virtual table and page its neighbor with their relationship both (parent and brother).

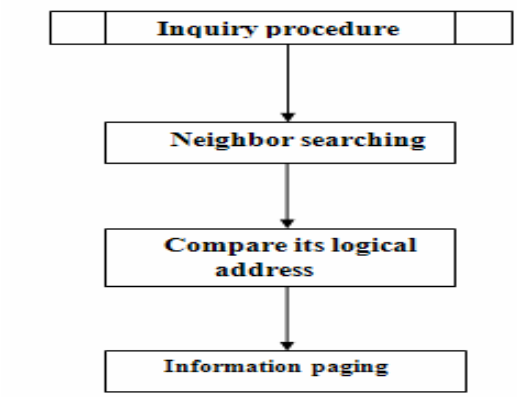

Figure 3: Inquiry Procedure

Algorithm:

STEP 1: Sensor node confirms the event occurrence first.

STEP 2: Sensor node reads its memory to acquire its neighbor's logical address.
STEP 3: If no other neighbors is near by then it put itself idle and starts inquiry procedure [because even though it is in temporary position].But this problem will not arise with our system because our postulated network fixed wireless.

STEP 4: If N=1 that means sensor node is having only neighbour, so it has to connect the node for sending data. After sending of data, acknowledgement will be received from node.

STEP 5: But if N>1, then our node of interest send the information through its parent node (or} If N>1 But parent node seems to be not there then it approaches shortest path approaches to send the data to its parent and get the Ack only from its near by parent. So we can assert that our sensor nodes always have an eye on its parent for sending the data.

STEP 6: Now the parent node is responsible for the data which must be router that has been explained already under the network configuration.

STEP 7: Parent node then goes to step 1 and repeats the same procedure.

This procedure continues unless or until data reaches the destination, which is nothing but control hub.
After the network configuration, an inquiry procedure is periodically performed, considering that some nodes disappear or newly appear in operating time. If there is no inquiry response from a node which had already been inquired before, it is considered that the node moved out from the range of the inquiring node or malfunctions.
Thus the inquiring node performs a series of three inquiries and if there is no response, finally removes the information of the node from its memory. If a node which had not been inquired before is newly inquired, the inquiring node makes a new record and pages the new node to exchange a packet which has logical address and other necessary information. The period for inquiring is normally set to 5 minutes. However, since each relay or sensor node must be connected to its parent node to operate normally, if its parent node is not inquired, such nodes periodically inquire every 40 seconds until their parent nodes are inquired. In the case of a sensor node, once it finds a parent node, it doesn't inquire until it loses its parent node. But, it does not matter because sensor nodes do not relay the packets from the other nodes. It also means that sensor nodes do not perform the inquiry procedure periodically. The sensor node needs to perform power management, so it doesn't inquire its parent node until its parent node disappears. If the sensor node inquires periodically, it consumes more power.
After all nodes go through the above network configuration procedure, they can achieve a network configuration based on the tree topology. As the depth of tree becomes deeper, the length of logical address becomes longer because an additional value is added to the rear of the logical address for identification

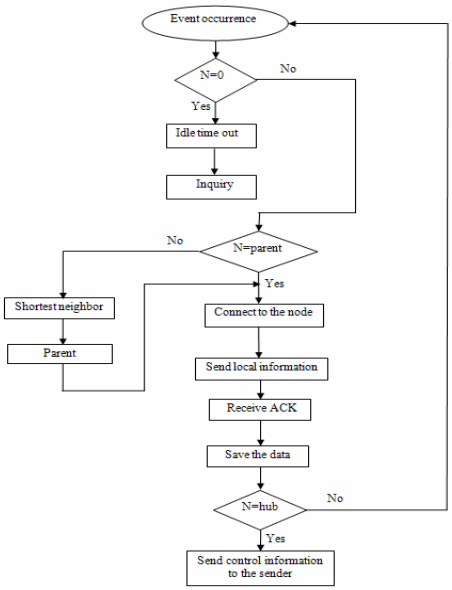

Figure 4: Flow chart for parent search routing

3.5.2 Node operation**.**

- External input event (e.g., a sensor detects an invader)
- We emulate this event by means of the on-off switch. The node detecting this event makes a Message packet corresponding to the event for reporting it to the local security control system. to send the packet, it searches the logical address of its parent node from the address table and then pages the parent node to send the packet.
- Retransmission timeout events: These events are further classified into the retransmission timeout for the link level ARQ and the retransmission timeout for the upper layer ARQ.
- Inquiry timeout event: This event occurs when the timer for periodic inquiry timeouts.
- Paging event: This event happens when a node is paged. The node performs different operations operations as follows according to the purpose of paging.

If it is paged to receive a Send OK packet, then it searches its transmitting queue which is maintained in anticipation of retransmission. And then it deletes the entry corresponding to the Send OK packet from the queue since the Send OK packet means that the transmission is successful.
If it is the final destination of the ACK packet when it is paged to receive an ACK packet, then it performs an operation similar to the case in which it is paged for receiving a Send OK packet. If it is not the final destination, however, then it just relays the ACK packet.
If it is paged when a new node wants to participate in the network and thus requests its information, then a packet which includes its logical address and other information necessary for connection is transmitted to the new node.
If it is paged when the local security control system wants to monitor its status, then it transmits a packet which contains its status information.
If it is paged due to a request for packet relay, then it transmits this packet to the next node on the multi-hop route. But the address of the source node is never

modified. This case happens only when it is a relay node. On the other hand, the control node also performs most functions of the sensor and relay nodes. Additionally it reports all the events received from the sensor or relay nodes to the local security control system via the UART interface and it checks, on demand of a system operator, the status of a specific node.

4. Experimental Results

The simulation of our proposed network with Bluetooth and Mobile nodes has been done to evaluate the performance that carries out two experiments.

We first measure the time taken for inquiring adjacent nodes and exchanging data between the inquiring node and the inquired node. The time consists of the inquiry time, the paging time and the data exchange time. We measure the period from the time when the inquiry procedure is initiated to the time when the data exchange is over. We assume that the inquiry procedure is performed at the network configuration stage. In this stage, each node continuously inquires for 4 seconds to find out its adjacent nodes, and then it pages the inquired nodes and exchanges data with the inquired nodes one by one for gathering the information which is necessary for network configuration. The result shows that the period is almost directly proportional to the number of adjacent nodes. It is because the inquiry procedure is continuously performed for 4 seconds regardless of the number of adjacent nodes and the time for paging and exchanging data takes about 0.8 seconds per each node.

Second, we measure the time taken to complete the data transmission between a sensor node and the control node. We measure the period from the time when the sensor node sends a packet to the time when it receives an ACK corresponding to the packet.

If the number of relay nodes is two, the number of total nodes involved is four and it means that the depth of the tree is also four. For each case, we perform experiments six times. As the depth of the tree increases, more time is needed to complete the data transmission. In addition, when adding one node, it takes about an additional 3 seconds.

From the experimentation of static nodes we have grasped that as the depth of the tree has been increased that dramatically increases transmission time, because the information has to cross several relay nodes on its way to control node.

Our postulations of movable relay nodes have solved this problem. According to our proposal depth of the tree can be increased with out increasing number relay nodes in such way that relay nodes come forward to sensor node.

From the experimentation we have observed that by using movable relay nodes inquiry time, paging time and transmission time have been considerably reduced.

4.1 Simulation Results

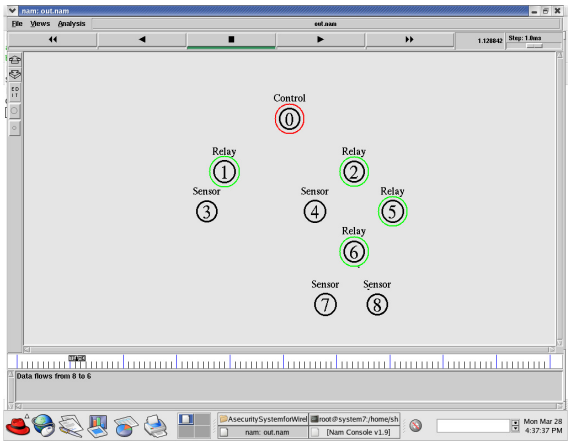

Figure 5: Simulation at 1.12 seconds for Bluetooth nodes

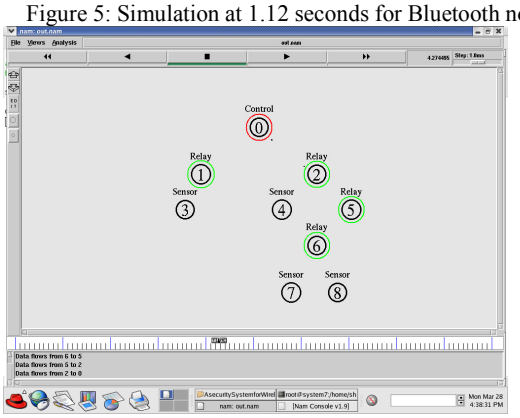

Figure 6: Simulation at 4.27 seconds for Bluetooth nodes

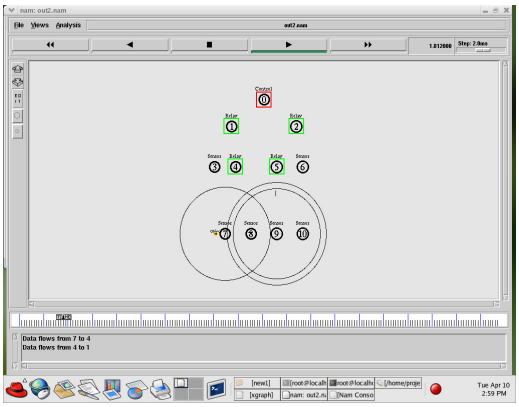

Figure 7: Simulation at 1.81 seconds for static nodes

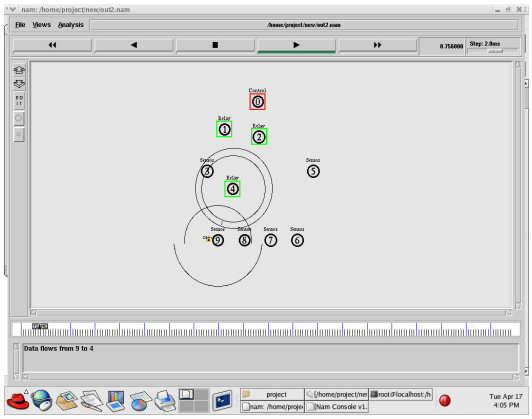

Figure 8: Simulation at 0.75 seconds for movable nodes

4.3.2. Output Graphs

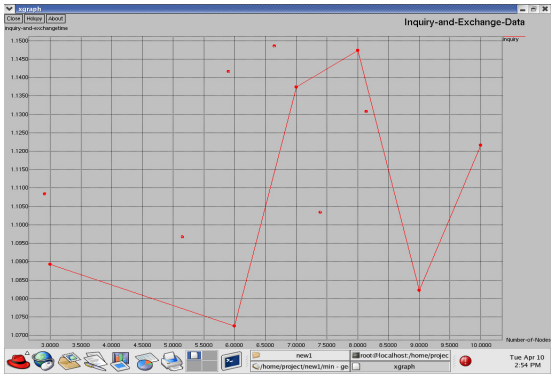

Figure 9: Inquiry and exchange time for static time for mobile nodes

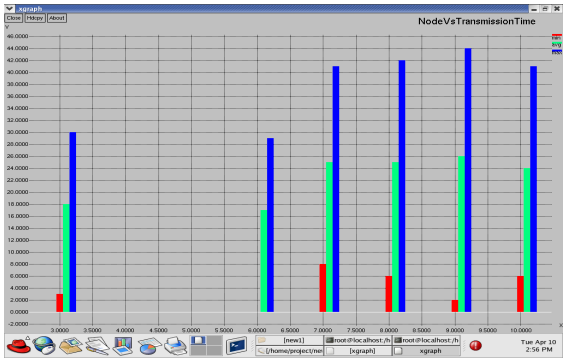

Figure 10: node vs. transmission static mobile nodes

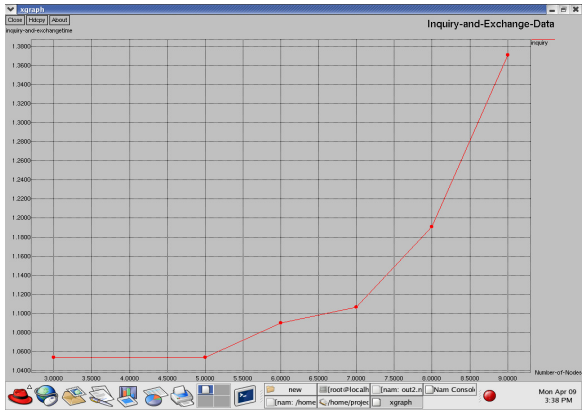

Figure 11: Inquiry and exchange time for movable time mobile nodes

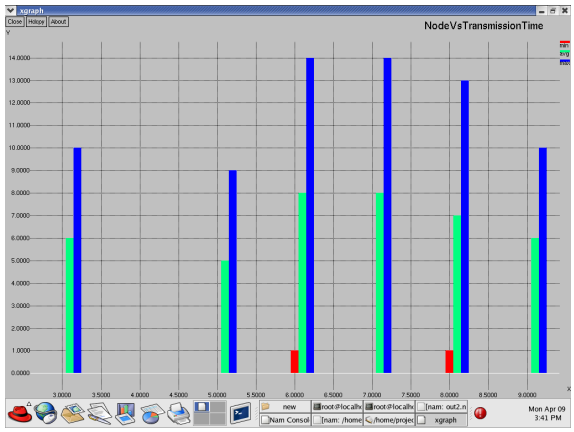

Figure 12: Node Vs Transmission for movable nodes

5. Conclusion

The difficulty in finding out the best and better path could be easily found out in our wireless mobile sensor network in the way of improving the security level at first. The topology here we have used is 'tree' and protocol for transportation is SCTP(stream control Transport protocol) and the algorithm what we have been using for routing 'parent searching'. Third stage of our project implies the movement of relay nodes which in turn reduces number relay nodes. The lesson we got from the experimentation is the reduction in inquiry time and data transmission efficiently because of the deployment of movable nodes.

References

[1] Soo-Hwan Choi, Byung-Kug Kim, Jinwoo Park, Chul-Hee Kang, Doo- Seop Eom " An Implementation of Wireless Sensor Network for Security System using bluetooth"IEEE TransactionsonConsumer Electronics, Vol. 50, No. 1, FEBRUARY 2004.

[2] YIh- Chun Hu, Adrian perrig, "A Survey of secure Wireless Ad-hoc Routing",IEEE Security & privacy, June 2004, Vol 2, Number 3, Page(s) 28-39.

[3] R. Stewar, Q. Xie, et al., "RFC 2960: Stream Control Transmission Protocol", The Internet Society 2000.

[4] Jianping Zou; Uyar, M.U.; Fecko, M.A.; Samtani, **"** SF - SCTP: An Extension of Stream Control Transmission Protocol to Support QoS", Networking, Sensing and Control, 2006. ICNSC '06. Proceedings of the 2006 IEEE International Conference on 23-25 April 2006 Page(s):780 – 785.

[5] Kamal, H.; Penoff, B.; Wagner, A **,"**SCTP versus TCP for MPI,Supercomputing, 2005. Proceedings of the ACM/IEEE SC 2005 Conference12-18 Nov. 2005 Page(s):30 – 30.

[6] Shaojian Fu; Atiquzzaman, M.,"Improving end-to-end throughput of Mobile IP using SCTP", High Performance Switching and Routing, 2003, HPSR. Workshop on 24-27 June 2003 Page(s):171 – 176.

[7] Fracchia, R.; Casetti, C.; Chiasserini, C.-F.; Meo, M , " A WiSE extension of SCTP for wireless networks",Communications, 2005. ICC 2005. 2005 IEEE International Conference on Volume 3,16-20 May 2005 Page(s):1448 – 1453.

[8] Joe, I **,"**SCTP with an improved cookie mechanism for mobile ad-hoc networks",.Global Telcommunications Conference, 2003. GLOBECOM '03,IEEE Volume 7, 1-5 Dec. 2003 Page(s):3678–3682.

[9] Dongkyun Kim , Jeomki Song , Joungsik Kim, Hongseok Yoo , Jungsoo Park , Cano, J.-. C, "The Applicability of SCTP to Mobile Ad HocNetworks " Advanced Communication Technology, 2006, ICACT 2006, The 8th International Conference, Volume 3, 20-22 Feb. 2006 Page(s):1979 – 1984.

[10] Alexander Rodzevski, " Creating a Wireless Sensor Network using Bluetooth Technology", TR-TS-765.

[11] Joe, I.; Kant, L.; SCTP with an improved cookie Mechanism for wireless networks through modeling and simulation**,**Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58thVolume 4, 6-9 Oct. 2003 Page(s):2559 – 2563.

[12] Caro, A.L., Jr.; Iyengar, J.R.; Amer, P.D.; Ladha, S.; Heinz, G.J., II; Shah, K.C.; SCTP: a proposed Standard for robust Internet data transport Computer Volume 36, Issue 11, Nov. 2003 Page(s):56 – 63

R.Kanthavel received his master degree in communication systems Engineering from Madurai Kamarajar University, Tamilnadu, India in 1999..He has published books for engineering students. He is currently working as Teaching research Associate in Government college of Engineering, Tirunelveli, Tamilnadu and his interests include Embedded systems, communication systems and computer networks.

L.Ganesan obtained his M.E. degree from government college of Technology,Bharatiyar University,Coimbatore,India and completed his Ph.D in Indian Institute of Technology, ,Kharagpur.He is currently working as professor and Head of Computer science and Engineering in Alagappa College of Engineering and Technology,Karaikudi,India.He has been doing continuous research and guiding in the disciplines of computer vision, image processing, Texture analysis, character reorganization and so forth. He has published many papers in reputed national and international journals.

R.Dhaya received her master of engineering in Embedded system Technologies from the Anna university, india. Currently she is a lecturer in the department of Information Technology in National Engineering College, Kovilpatti, India.Her interest include wireless sensor networks and Real time systems.