International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Proposed Security Framework Module of Agent Communication Manager for Mobile Ad Hoc Network

Rajesh Kumar[1], S. Niranjan[2]

[1]Research Scholar, Mewar University Rajasthan, India

[2]Professor, Computer Science & Engineering Department, GITAM, Kablana Jhajjar, India

Abstract: ***In this paper we are going to propose security framework module of Agent communication Manager for MANETS. Security framework is a major concern for any type of communication system. The proposed framework describes the concept of how mobile agents will interact with each other, various security threats and how to resolved issues concerning for the efficient transreception of information. The proposed security framework emphasises on agent communication module which was earlier designed, besides communicating among devices, communication flow and interaction. Here we are introducing a security manager for agent communication that support the dynamic as well the static infrastructure according to the nature of the problem. The proposed security framework is the advancement in the already existing architecture for agent communication manager in MANETs.***

Keywords: Agent communication manager (ACM)**,** Broadcasting Module (BM), Comparator (CPR), Directory Facilitator (DF), Service Data Base (SDB), Service Provider Module (SPM)

1. Introduction

The advent of mobile agent technology (MAT) has caused an appreciable impact on the functioning of information & communication engineering and gaining more and more attention in areas like research, commercial worlds etc. Mobile agent is defined to be an autonomous software entity able to interact with its own and in other environments. There are lot of expectations put on these agents but their large scale use is still waiting due to immaturity of agent technology is that we have not able to make it secure enough to fulfill the expectations. While agents may solve many problems typical to these environments, agents require special support from underlying architecture [4].

The mobile agent can be thought of as a software program which travels from one platform to another in order to get its work done, during this process it carries its state and data with itself and resume its execution from the state it had left on the previous platform [7]. The reason for using mobility is the improved performance which can be achieved by moving the agent closer to the new host, where it can use services locally. Now a day's agent and their platforms are designed to operate in fixed network or we can say in the fixed infrastructure environments, therefore they do not yet operate on dynamic environment the wireless environment here we proposed architecture for agent communication manager in mobile ad-hoc network (MANET) can operate in dynamic infrastructure as well as in static environment or we can say in full duplex mode [2].

In this paper we concentrate on the security framework for mobile agents. The security framework is then applied to the data transmission and reception and task will be completed by security manager. The security architecture is divided into different parts like comparator, service provider module, linker, broadcasting module, transmission module, agent control system, directory facilitator, router proxy, security manager.

2. Related Works

Existing ACM ARCHITECTURE

The architecture designed [15] was compatible with FIPA specification for conforming to maintain communication flow for ease of interaction module named AC Manager (ACM) was added. Each module on the platform was able communicate to others via Message Transportation System. But there was no provision of secure communication. The ACM consists of Comparator, SPM, Linker, Transmission module, Broadcasting module, ACS and DF Controller, Router and Proxy as shown in fig1. Each Module is explained as follows.

2.1 Comparator (CPR)

CPR knows about the devices (either it may be mobile or fixed), hardware performance and compare it with other devices in the network. By this, SPM decides the next SPM. After the system is composed, the CPR of the SPM manages the priority of the SPM by performance of others.

2.2 Linker (LKR)

When the device connects to the MANET, the LKR finds the SPM in the network and registers its own agents and services to the SPM, performs the disconnection to the other nodes in advance and recognizes that the other node is disconnected or the SPM of the system has changed. In addition, when it communicates with the SPM, it transfers a list of connected nodes.

2.3 Broadcasting Module (BM)

To hand over the role of the SPM, the BM performs backup of agents and service data to the other Services. The BM runs only on the SPM or backup devices.

2.4 ACS and DF Controller

If disconnection of the SPM is recognized by CPR and the device should be next SPM using the priority order, then ADC register agents and service information to its own ACS and DF and executes the agents. It runs when a change in the SPM is needed.

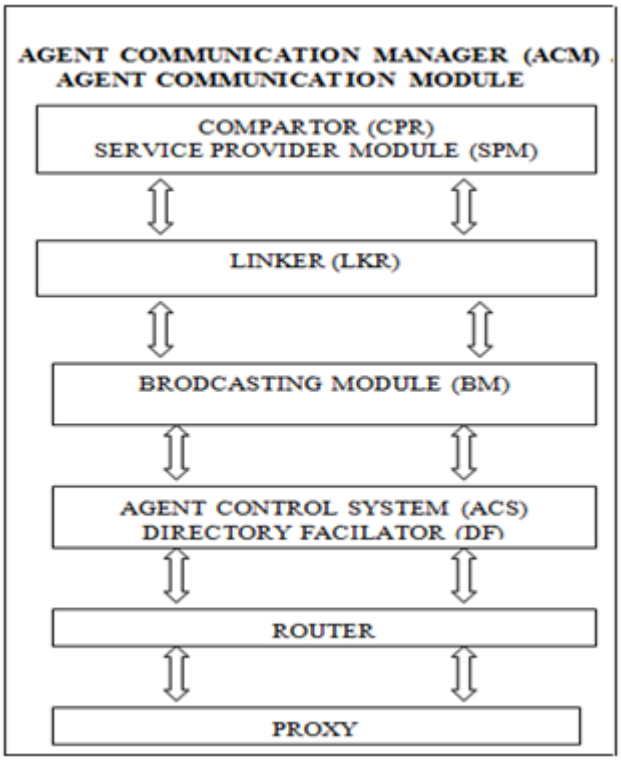

Figure 1: Architecture for Agent Communication Manager

2.5 Router (RT)

The RT is responsible for routing paths between untraceable nodes and sending messages through the paths.

2.6 Proxy (PR)

The PR takes charge of proxying agent services. The PR registers transmitted agents from the requesting device to the ACS and DF, executes them, generates results, and communicates with the requester.

2.7 ACS and DF

The ACS and the DF are agents responsible for agent management service, FIPA specification [7]. The ACS is a mandatory element of the agent platform. It will exist only once on a single agent platform. It function is to registers and deregisters agent on the Agent ID directory. It also manages agent transfers on an inter-platform when it is supported. For producing yellow pages service to the other agents DF component is essential. Each agent platform must have at least one DF component and multiple DFs also exist within an agent platform.

2.8 JADE – LEAP

The Java Agent DEvelopment Framework (JADE) is a software framework implemented in Java. The purpose of the JADE is to simplify multi agent system implementation, compatible with the FIPA specification. To use it on mobile devices, the JADE – Lightweight Extensible Agent Platform (JADE - LEAP) is developed. It enables agents to be executed on light weight devices such as cell phones. It is developed to run on mobile device supporting sufficient resources and processing power without any modification and it uses wireless networks [14]. It is one of the most popular mobile agent systems but cannot be used where TCP/IP is not supported.

2.9 Bluetooth Devices for Agent Network (BDAN)

This system provides agent service on personal mobile devices using the Bluetooth protocol. BDAN consist of mobile and fixed devices that are Bluetooth enabled [12]. When mobile devices access and request a service from a fixed system, it creates an agent for managing them, which interact between agent and user. The BDAN can provide agent service where TCP/IP is not supported, but must have a fixed infrastructure like JADE-LEAP terminals.

- Provides Broadcasting and Transmission Services among mobile devices without a fixed infrastructure.
- It also facilitates the services of full duplex mode.
- It also maintains the service provider manager through another device when the current device disconnects from MANETS (Mobile Ad-hoc Networks).
- Expected to support agent communication between remote and untraceable nodes.
- Agent Control System and Directory Facilitates used for Single as well as Multi Agent System.
- It also support other modes like Bluetooth, Infrared and wireless transmission etc [9].

3. Proposed Security Framework For ACM

3.1 The proposed security framework emphasis on the following points:

1. Establishment of communication.
2. Communication flow between or among devices.
3. Different components of framework for mutual interaction (amongst themselves).
4. Interaction with the Web services.
5. The sequence of flow or standard operational procedure for the task.
6. Process of authentication.
7. What are the methods for preventing security threats?
8. Tools required for security frame work as well as the interaction among them.
9. Function of security mechanism.

3.2 Main Components of security framework are as follows:

1. D1, D2, D3 and D4 Devices which includes any compatible device such as (Personal Computer, Desktop computer, Laptop, PDA, Mobile etc.)
2. User Interface
3. Security Manager
4. BM: Broadcasting Module.
5. DF: Directory Facilitator
6. ACS: Agent Communication System.
7. SDB: Service Data base
8. Router Proxy
9. Linker / Connecting Media
10. Web / Internet
11. CPR : Comparator

Note: The all devices which are above mentioned are communicating with each other in Mobile agent ad-hoc networks.

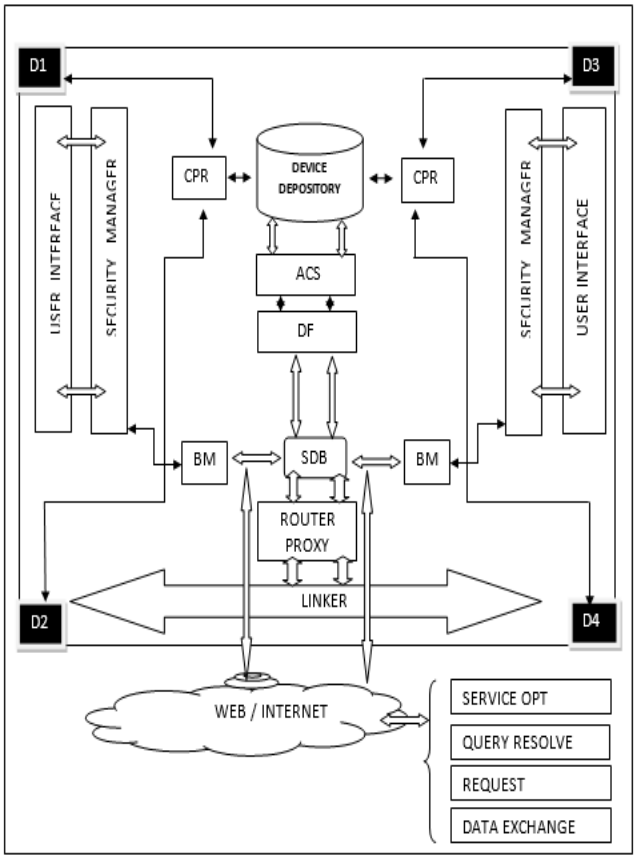

Figure 2: Detailed diagram of proposed security framework.

3.3 The working as well as the operational environment of proposed security framework is as follows:

- First of all, any of D1, D2, D3, and D4 devices we already explained above are establishing a connection between any two of the devices or and among themselves.
- The concerned device first connects with the user interface and the user interface provides the essential things required to establish the connection amongst the devices in the network.
- Then Security manager comes it provides the security as well as the authentication, authorization on that particular network.
- After Security Manager the task of Comparator starts it checks the compatibility with the network for particular device as well as the communication established between the Fixed and Mobile devices compatibility.
- Device Depository maintains the log reports of the devices in which the communication is established.
- The Agent Communication System DF
- The ACS and the DF are agents responsible for agent management service, FIPA specification. The ACS is a mandatory element of the agent platform. It will exist only once on a single agent platform. It function is to registers and deregisters agent on the Agent ID directory. It also manages agent transfers on an inter-platform when it is supported. For producing yellow pages service to the other agents DF component is essential. Each agent platform must have at least one DF component and multiple DFs also exist within an agent platform.
- SDB stands for Service database which plays a vital role among the Broadcasting module, Directory Facilitator and the Router Proxy.
- SDB works like a interface among the above mention components, it also passes the information from one component to other component.
- The LINKER plays the Linking task among the components.
- The Connecting Media may be BDAN: Bluetooth Device for Agent network, WSN: Wireless Sensor Network, Wired, and WIFI. It depends upon the nature of problem for which the concerned connection is formed.
- The Web as well as the Internet resides between the BM and SDB and their functions frequently change according to the nature of problem or we can say the task of the problem.
- The Web / Internet also deals with the important services like Service opt, Query resolve, Request Processing and Data Exchange.
- The above mention frame work depends on the number of devices which interacts with each other and the nature of problem of the task which is resolved by them.

4. Security Management

The purpose of security manager is to control access to the external resources like file or network connection. This can be achieved in such a way that the Java API supports the security policy by asking the security manager for permission before any possibly of unsafe action taking place. Asking for permission can be carried out by invoking check methods on the security manager object. For example, when a Sever Socket receives a connection request, the check Accept method in the security manager is called to check if it is allowed to open a new socket to the specified host address and port number. The security policy that is followed by the security manager is defined in the policy file. The policy file, on its behalf, can be configured by the policy tool, which is a graphical user interface that assists a user in specifying, generating, editing, exporting, or importing a security policy. The tool can be run from the command line [9].

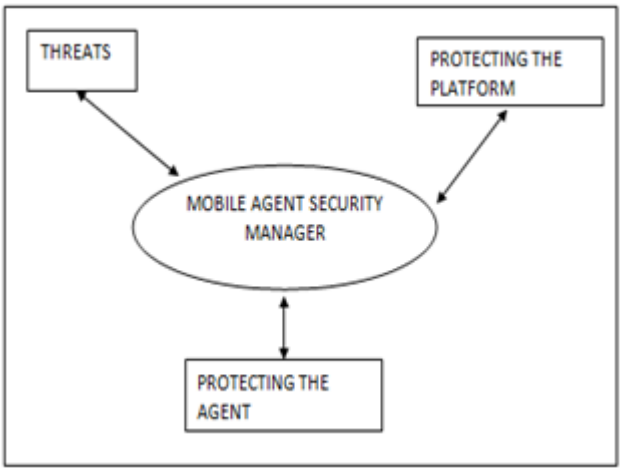

Figure 3: Security Manager

Another important security tool i.e. provided by Java is the keytool. It is a key and certificate management tool. With the keytool, user can administer their own public/private key pairs and associated certificates. Also the certificates referring to the trusted communication parties can be managed by the keytool. User's own keys, certificates and certificates from trusted parties are all stored in the same key store from where keys can be referenced by an "alias". This key store is protected with a password from unauthorized users. In addition, privates' keys are also protected with individual passwords to guarantee that they do not unintentially fall in to the wrong hands. The keytool can be run either from the command line or the user can create their own security application using KeyStore class provided by the java security package. With the keytool user can display, import and export X.509 certificates. It allows the user to specify. Any key pair generation and signature algorithms supplied by any of the registered cryptographic service providers [10].

4.1 Mobile Agent Security Threats and Protection

Although security plays a very important role in developing mobile agent systems, many of them are developed without a deeper knowledge of security, leaving it open to be taken care of in the future. However, in order for mobile agent technology to make a breakthrough in the area of commercial applications and gain widespread use, security issues need to be first addressed properly [8]. Security and openness are often said to be opposite in a sense that it cannot have both of them at the same time. There can be a situation as to how the same agent can be both secure and mobile. The answer is simple, mobile agent do not have to be perfectly mobile and they are not also meant to be fortresses that can hold massive attacks. They are a combination of both on a suitable scale and the relation of those usually depends on the task that agent is intended for.

4.2 Threats

Many threats in mobile agent systems can also be found in traditional distributed network environments. However, introducing mobile agents significantly broadens the opportunities for misuse. A migrated mobile agent residing in a remote platform also raises numerous security issues to be taken care of. To be able to protect agent platform and mobile agents, which move between them, we have know exactly what kind of threats an agent system faces. These threats can be divided in to four main categories [11]

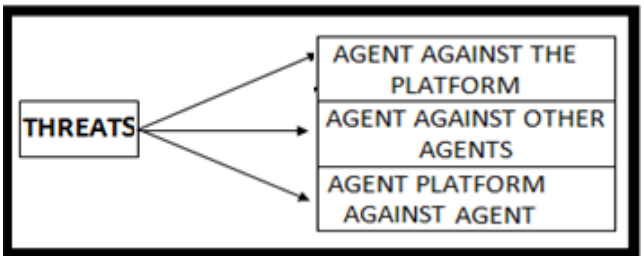

Figure 4: Security threats of mobile agent system

4.2.1 Against Platform

The attacking agent has two main ways to inflict harm to the agent platform. An agent can try to gain unauthorized access to the information inside the agent platform, or an authorized agent can try to cause harm to the platform. Unauthorized access can be acquired by masquerading, which means that an agent pretends to be some other agent that is trusted by the platform.

When unauthorized access has been gained, an agent has several ways to cause serious harm to the platform, for example, by revealing classified information. It is tougher to protect the platform an agent that has authorized access to the platform and thus is trusted.

An agent can attack the agent platform even without gaining access to it. This can be achieved with a denial- of – service (DOS) attack, which is used to deny platform services to other agents by exhausting the platform's computational resources [11]. The denial- of –service attack can be performed, for example, by creating an innumerable amount of malicious agents trying simultaneously to log on to the agent platform, with their only intention to exhaust it, and thus preventing benevolent agents accessing the platform.

4.2.2 Agent for Agent

A malicious agent has several approaches to attack other agents. It can take action to falsify transactions, eavesdrop on conversations, or interface with an agent's activity [11]. One of the threats is masquerading, where an agent pretends to be an agent other than it really is, causes some kind of harm to the agent system and then leaves the accusations of the community to the real agent

4.2.3 Agent Platform against Agents

To protect an agent from the agent platform is by far one of the most difficult and discussed problems in the field of mobile agent security. It is usually referred to as a malicious host problem and occurs when the agent has arrived at the remote platform. After that the host platform loses its control over the agent and little can be done to stop the remote platform from treating the agent as it likes [8]. The remote platform can easily, for example, check the information that the agent is carrying, deny requested services, alter the agent's data or even terminate the agent completely [11].

Masquerading is one possible threat carried out by a malicious platform that falsely pretends to be another trusted

platform. It is directed towards mobile agents, which are not yet inside platform and thus can be deceived about the destination where they will migrate to. Consequently, agent will log themselves onto the malicious platform believing that they have arrived at some other platform that is trusted. Once the fake platform has succeeded in deceiving, it has several other possible attacks that may be launched at agents residing in it.

4.3 Protecting the Platform

The agent platform is vulnerable to attacks by malicious platforms, malicious agents and other malicious entities unless it takes proper action to protect itself. A number of security mechanisms have been introduced in various works concerning mobile agent security. Despite the fact that protection of the agent platform and the agent itself are concerned separately here, the overall security of the agent system is their integration, and should be developed simultaneously.

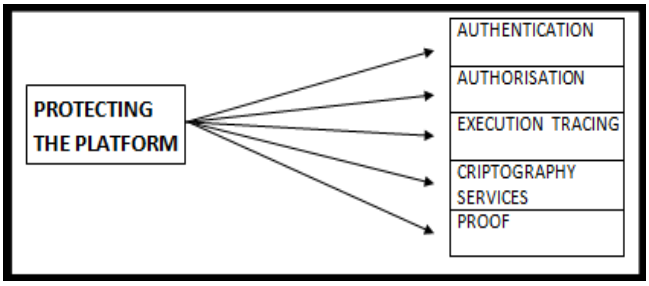

Figure 5: Protection of Platform

4.3.1 Authentication

When a migrating agent arrives at an agent platform, it is an important part of the platform's security to authenticate the incoming agent and thus clarify the agent's identity. The platform can try to associate an agent with the agent's original author, the agent's sender or both. Authentication is commonly carried out using digital signatures. A public key cryptography is usually used for signatures [3]. Every mobile agent that migrates to the agent platform, including mobile agents that are returning to their home platform has to be authenticated, otherwise access has to be denied.

4.3.2 Authorization

Agent platforms usually have different levels of access rights, which are based on the security policies which are already fixed. The decision on the level of access right and thus defining which resources are required is given by the system administrator [15].

4.3.3 Execution Tracing

It is a mechanism for providing security mainly for mobile agents its actions are mostly executed by agent platform and therefore it is considered under platform security. Execution tracing is a technique for detecting unauthorized modification of an agent [1].

4.3.4 Cryptographic Services

It has two purposes it is used by the agent platform for encryption and decryption for inter agent platform communication. It also provides an encryption services for residing agents.

4.3.5 Proof

Proof is a mechanism that is used in agents to save its state and data when it travel across the network or we can say for inter agent platform proof is required.

4.4 Protecting the Agents

Mobile agent has to be designed paying attention to the idea that a text can also arise from the execution environment. Security risk causes different problems depending upon how far from the home platform an agent is allowed to move.

- **Path History**: is to maintain an authenticable record of mobile agents.
- **Partial result encryption:** It describes how to protect confidential information that one platform has received from other platforms.
- **Proof of agent identity:** Proof is a mechanism for providing assurance of a mobile agent identity to the agent platform [3].

5. Conclusion

The proposed architecture satisfies the conditions essential for broadcasting as well as transmission with improved level of security. It also works on Single Agent as well as Multi Agent system. Another feature of this architecture is that it supports dynamic infrastructure as well as static infrastructure. The security manager helps in protecting the platform; agents from various threats by adapting different security mechanisms. This proposed security framework for agent communication manager will be compatible with new protocols for different modes like Bluetooth, Infrared, wireless & wired media according to the requirement of network for efficient communication.

6. Future Scope

Instead of security weakness in the implemented agent system, the future of mobile agent systems can be seen as promising, however, a lot of work has still to be done. In particular, if we can answer how the mobile agent can be protected efficiently while it resides in a remote platform. If the answer can be found, based on trusted platforms can be ignored, which will open a number of opportunities. Security mechanisms such as proof of agent identity, partial result encryption are small steps in the right direction, and also many other mechanisms have been proposed in order to improve the mobile agent security.

References

[1] Vigna, G. (1997 Protecting Mobile Agents Through Tracing. In: 3rd ECOOP Workshop on Mobile Object Systems Jyvaskyla, Finland. PP 137-153.
[2] Moreh, Jahan, "Publish & Subscribe: The Power behind Interactive Push Technology," Distributed Computing, 1:2, January/February, 1998, PP. 23-27.
[3] Tschudin, C.F. (1998) Mobile Agent Security. In: Klusch, M. (Ed.) Intelligent Information Discovery and management on the Internet. Springer-Verlag, Germany. PP. 431-445.

[4] Heikki Helin_, Heimo Laamaneny, Kimmo Raatikainen " Mobile agent communication in wireless network "European Wireless'99/ITG'99. October 1999, PP. 211-216,
[5] IEEE Foundation for Intelligent Physical Agents (FIPA). Agent Management Specification. http://www.fipa.org/specs/fipa00023/SC00023K.pdf
[6] JADE. Java Agent DEvelopment Framework. http://jade.tilab.com/
[7] Java Agent Development Framework (JADE). JADE-LEAP User Guide. http://jade.tilab.com/doc/LEAPUserGuide.pdf
[8] Borselius, N. (2002) Mobile Agent Security. Electronics & Communication Engineering Journal, Vol.14, No. 5, PP 211-218.
[9] Jamie Lawrence, "LEAP into Ad-Hoc Networks, "Workshop on. Ubiquitous Agents on embedded, wearable, and mobile devices, Bologna, 16th July, 2002.
[10] Gong, Li (15.12.2003) Java Security Architecture (JDK 1.2). URL: http://java.sun.com/products/jdk/1.2/guide/security/spec/security-spec.doc.html
[11] Jansen, W.A. (20.1.2004) Mobile Agent and Security. URL: http://citesser.nj.nec.com/jansen99mobile.html
[12] Alessandro Genco, Salvatore Sorce, Giuseppe Reina, Giuseppe Santoro, "An Agent- Based Service Network for Personal Mobile Devices," IEEE Pervasive Computing, Vol. 05, Issue no. 2, Apr-Jun, 2006, PP. 54-6.
[13] Object Management Group, NEEDAM MA, Agent Technology Green Paper 1, Sept 2010, PP. 8-11.
[14] Danny B.Lange and Mitsuru Oshima,"Programming and Developing Java Mobile Agents with Aglets". (Addison Wesley publication). Reprint 2012
[15] Yashpal Singh, Rajesh Kumar and S. Niranjan, "A Proposed Architecture for Agent Communication Manger in Mobile Ad-Hoc Network." IFRSA International Journal Of Electronics Circuits And Systems, Vol., 1Issue 1, Feburary 2012, PP. 44-47.

Author Profile

Rajesh Kumar was born on 8th Sept.1983, in India. Got bachelor degree from Hindu College Sonipat affiliated from MD University Rohtak, Haryana in 2005, First post-graduation (MSc VLSI) from Vaish PG College, Rohtak affiliated from MDU Rohtak with 68.5% in 2008, Second PG Degree (M.Tech. ECE) from Vaish Engineering College Rohtak, affiliated from MDU Rohtak with 75.45% in 2010 and area of research was VLSI Technology and published four papers in international and national conferences. Joined PhD programme under Mewar University, Chhittorgarh, Rajasthan, India in 2011. Area of research in PhD: Mobile Agent Technology in the topic, "Design and Development of Advance Security Systems of an Mobile Agent Based Architectures" and published two research papers in reputed international journals. Besides this attended four FDPs & three workshops.

Niranjan S was born on 4thApril 1955 in India. Graduated from University College of Engineering, Sambalpur University in 1978 in Electronics & Telecommunication Engineering, worked as asst Engineer under State Govt and Ex. Engineer under State Electricity Board working for Power line Carrier Communication Systems, Protective relaying, telemetry and LFC Systems. Master's Degree from IIT Kharagpur in 1987 in Computer Engineering. Worked in the areas of Parallel Processing. Performance characterization of parallel Programs under variable and uniprocessor environments, worked towards the development of a machine and hand printed Oriya Character Recognition System. PhD from Utkal University. Area of work is Study and issues of mobile Computing Algorithms. He has also worked in the areas of Load Frequency Control in deregulated Scenarios and study of various non linear models of interconnected power Systems including GRC and other stochastic conditions. His current research areas include ECC based cryptographic applications, mobile ad-hoc sensor networks.