ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

Identification and Isolation of Replica Attack using Risk Aware Response Mechanism

Mr. K. Rajkumar[1], Dr. P. Ganeshkumar[2], P. Senthilkumar[3]

Associate Professor, Dept of IT, PSNA College of Engineering &Technology, Dindigul, Tamilnadu[1]

Professor, Dept of IT, PSNA College of Engineering &Technology, Dindigul, Tamilnadu[2]

Associate Professor, Dept of IT, PSNA College of Engineering &Technology, Dindigul, Tamilnadu[3]

Abstract: Mobile ad hoc networks (MANETs) are a set of mobile nodes which are self-configuring and connected by wireless links automatically as per the defined routing protocol. The key feature of MANETs is the absence of a central management agency or a fixed infrastructure. Since the most devastating damage to MANET is caused by routing attacks they have received considerable attention. In the existing system, a risk-aware response mechanism is proposed to systematically cope with routing attacks in MANET. The intrusion detection systems (IDS) used here have limited response mechanisms that are inadequate given the current threat. In the proposed system, along with the existing system approach, a more efficient detection algorithm for detecting replica attacks in MANET is proposed. Replica Attacks is an attempt by the adversary to add one or more nodes to the network that use the same ID as another node in the network. Location Information Exchange protocol and Time Domain Detection & Space Domain Detection Scheme both to detect node replication attack in the network. The advantage of this system will be increased detection accuracy and reduced network damage.

Keywords: Mobile ad hoc networks, replica nodes, intrusion response, adaptive decision making.

I. INTRODUCTION

A wireless ad-hoc network is a collection of mobile/semi-mobile nodes with no pre-established infrastructure, forming a temporary network. Each of the nodes has a wireless interface and Laptop computers and personal digital assistants that communicate directly with each other communicates with each other over either radio or infrared. are some examples of nodes in an ad-hoc network. These nodes are mobile and also consist of stationary nodes. Semi mobile nodes will deploy relay points in areas where relay Figure 1 show a simple ad-hoc network with exactly three nodes. Two nodes are not in the transmitter range of each other. In order to communicate these two outermost nodes, middle will be used for forwarding packets between these two nodes. The middle node will perform router's task. Now all nodes together form ad-hoc network. An ad-hoc network uses no centralized administration. This network will not collapse because one of the mobile nodes moves out of transmitter range.

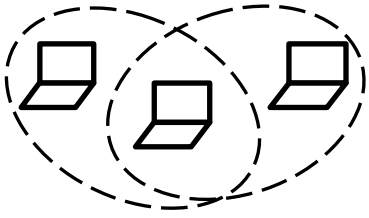

Fig.1

Nodes must be able to enter/leave the network due to nodes have limited transmitter range. To reach the other nodes, multiple hops will be needed. Thus, every node wishing to participate in an ad-hoc network must be willing to forward packets for other nodes. Any compromised nodes under the adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks.

MPR of a node. Or, the attackers can give wrong information about the topology of a network (TC message) in order to disturb the routing operation. Decisions based on the evidences and its own individual benefits. Therefore, some nodes in several work [1], [2] addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from its behaviours. Such response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET, improper countermeasures will lead to unexpected network partition. It will additionally damages infrastructure of the network. For the above problem, flexible and adaptive response will be investigated.

.

II. BACKGROUND

In existing systems, D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by various other engineering fields

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

[7], [8], where precise measurement is impossible to obtain or expert elicitation is required. D-S theory support Dempster's rule of combination (DRC) to combine several evidences together with probable reasoning. However, as identified in [9], [10], [11], Dempster's rule of combination has limitations, such as treating equally without differentiating every evidence and considering priorities among them. To solve this limitations in MANET intrusion response scenario, a new Dempster's rule of combination with a notion of importance factors (IF)[3] in D-S evidence model was introduced.

Here a risk-aware response mechanism was proposed to systematically cope with routing attacks in MANET, but now adaptive time-wise isolation meth- od is proposed. The risk-aware approach is based on the extended D-S evidence model. Then to simulate the proposed concept they used a proactive MANET routing protocol called Optimized Link State Routing protocol (OLSR).

Based on the behavior of attackers, these attacks can be classified into passive or active attacks. Again it is categorized as outsider and insider attacks. In routing packet attacks, attackers could not only prevent existing paths from being used, but also spoof nonexistent paths to lure data packets to them.

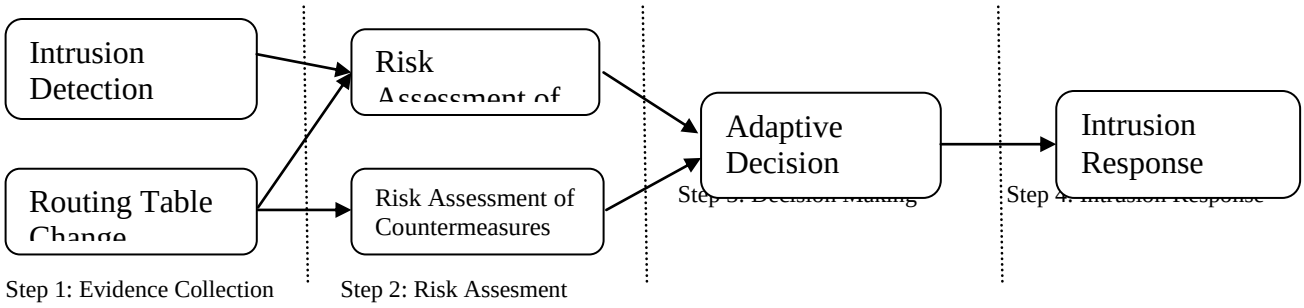

Figure 2: Block Diagram of Intrusion Detection System

Typical routing attacks consist of black hole, fabrication, and routing packets with modification in fields. All these attacks could lead to serious network dysfunctions. Therefore, the attacker can abuse the properties of the selection algorithm as MPR. The worst case is the selected attacker is the only MANET may isolate the malicious node, but others will be in cooperation with high dependency relationships. The disadvantages of the existing systems are :At present , the intrusion detection systems (IDS) have limited response mechanisms that are inadequate for the current threat.

III RISK AWARE RESPONSE

Here an adaptive risk aware response mechanism based onquantitative risk tolerance and risk estimation. Instead of applying simple binary isolation, new approach provides isolation mechanism in a temporal manner based on the risk

IDS carried out only the risk assessment techniques and isolation procedure. IDS has focused on better techniques for intrusion detection, intrusion response remains principally a manual process.

In this paper we detect replica attacks in manet and then isolate them using a adaptive decision making approach. Replica attack is an attempt by the adversary to add one or more nodes to the network that use the same ID as another node in the network. These nodes have all valid security credentials and therefore can easily launch various attacks (like blackhole attack, fabrication, eavesdropping, sinkhole attack, etc.) inside a network. In MANET all communication relay on message relay/forwarding. Replicas may misguide the communication in a network and there by jam the communication.

Detecting replica attacks is very crucial in MANET due to high node mobility. Two replication detection schemes such as Time Domain Detection and Space Domain Detection are proposed. Also, a protocol called the Location Information Exchange Protocol is used for replica attack detection.

In this protocol, whenever two nodes meet each other both will exchange some information they are, Time & location at when they meet each other, Challenge key, which is having least index and unused in challenge chain and Signature of that node signed using public key. Information exchange process should happen with all

nodes the node meets on the way. If anyone fails, from the knowledge of the neighborhood node can easily detect the abnormal silence of the replica node. This technique can easily detect a node reposting wrong time and location.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

value. The risk assessment is performed with the extended D-S evidence theory for both attack and corresponding countermeasures to make more accurate response decisions illustrated in figure 2.

3.1 Overview

Because of the infrastructure-less architecture of MANET, our risk-aware response system is a distributed system that is each node will makes its own response decisions base on the evidences and its own benefits. So some nodes isolate the malicious node, but others nodes will keep in cooperation due to high dependency relationships. The risk-aware response mechanism is divided into the following four steps shown in figure 2.

Evidence Collection:

In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value,and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.

Risk assessment:

Alert confidence from the routing table and IDS changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated well during a risk assessment phase. From the risk of countermeasures and the risk of attacks, all the risk of an attack will be figured .

Decision making:

The adaptive decision module provides a flexible response decision-making mechanism that will consider risk tolerance and risk estimation. For adjusting temporary isolation level, a user have to set various thresholds to fulfill the goal.

Intrusion response:

Output taken from risk assessment and decision making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner.

The drawbacks are:

- During communication, replica is forced to generate challenge key along with their movements by which replica attack is easily detected by the proposed scheme.
- No limitation on number of replicas in a network.
- Use of 1-way hash function results, low computation overhead.
- It provides high detection accuracy.

IV MODULE DESCRIPTION

The modules are:

- Network formation
- Attack model
- Protocol implementation
- Attack isolation
- Performance analysis

4.1 Network formation

The simulation work has been done with The Network Simulator ns-2, Version 2.29. In the simulation 300 nodes are randomly distributed within the network field of size 1000m*1000m.

4.2 Attack Model

To prove our model we need to formulate an adversary model in our network. Adversaries are intruders in our network they do false things against the protocol. The adversary model here for monitoring the network activities such as record data, time and size of the packet sent over the network also it observes the source and destination nodes id for disrupting the packet transmission.

4.3 Protocol implementation

Detecting replica attacks is very crucial in MANET due to high node mobility. Two replication detection schemes such as Time Domain Detection and Space Domain Detection are proposed to detect node replication attack in our network.

Location Information Exchange Protocol

Whenever two nodes meet each other both will exchange some information they are - Time & location at when they meet each other and Challenge key, which is having least index and unused in challenge chain. Information exchange process should happen with all nodes the node meets on the way. If anyone fails, from the knowledge of the neighborhood node can easily detect the abnormal silence of the replica node. With this technique can easily detect a node reposting wrong time and location.

In this detection protocol, there are some conditions that is required to be taken . They are:

- At any specific time, Location and challenge presence should be unique.
- Also it should be in consecutive order with the time coordinates.
- Validation of two messages that a node ‘v’ and ‘w’ have received from ‘u’ should be such that, the challenge should follow the ordinal order of u’s challenge chain based

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

on the time. And the distance between the location mentioned in the messages must be less than or equal to the maximum possible distance 'u' can traverse.

- Also, the no. of nodes ''u meets during that time interval should be less than or equal to the maximum possible nodes that it can meet.

Time domain detection

Using this algorithm going to check whether the node is intrusion or not at a particular period of time. For that node is compared with all other node in the network such that:

If both nodes met during that time means the message it got from that node is transferred to the nodes that are in the location mentioned in that message, for reference to other nodes and their consistency is checked. If it violates our considerations returns as attack is detected.

If not it won't report about the node 'u'.

Space domain detection

Here two nodes are arbitrarily chosen as witness nodes. The witness nodes will exchange information that each have in table. The two nodes that act as witness nodes, randomly select some nodes for checking. If there are any irregularities in the information exchanged then, the node under the observation of the witness nodes will be a replica node.

4.4 Attack Isolation

If the frequency is high in the attack, then severe response action must be taken. Our risk-aware response module will achieve this objective by reducing the values of risk level threshold and narrowing the range between two risk level thresholds.

4.5 Performance analysis

Here the performance of the routing protocol is evaluated using the NS-2(version 2.29) stimulator. Various network parameters of the proposed system is analyzed and compared with the network parameters sof its predecessors. Some of the parameters analyzed are:

- Byte Overhead & Packet Overhead
- Mean Latency
- Packet Delivery Ratio
- Routing Cost

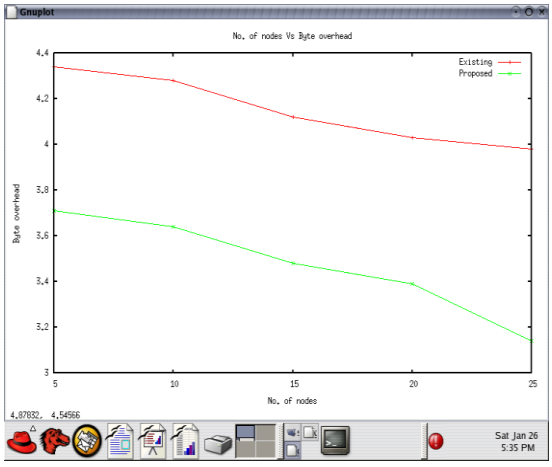

Figure 3: No. of nodes Vs Byte Overhead

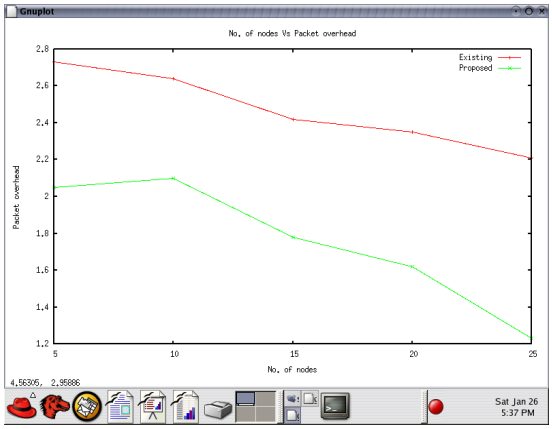

Figure 4: No. of nodes Vs Packet Overhead

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

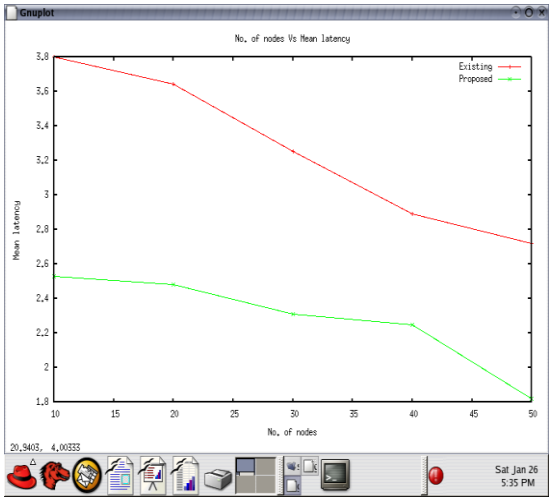

Figure 5: No. of nodes Vs Mean Latency

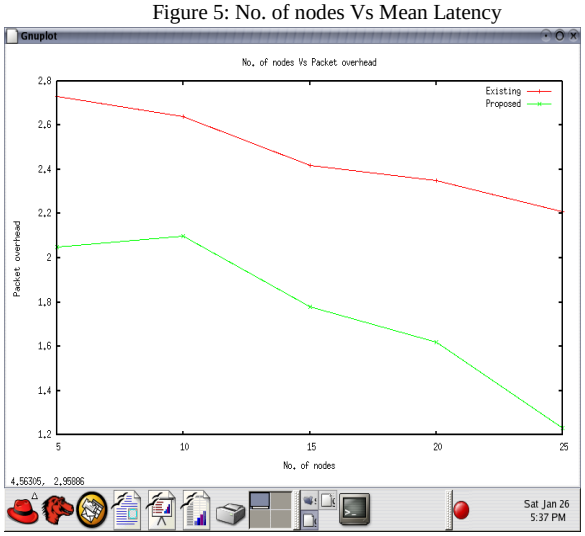

Figure 6: No. of nodes Vs Packet Delivery Ratio

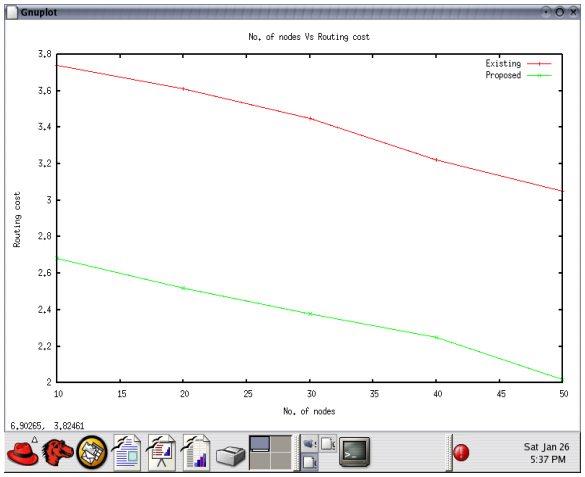

Figure 6: No. of nodes Vs Routing Cost

5. RELATED WORK

Some research efforts have been taken to seek preventive solutions [11], [12], [13] for protecting the routing protocols in MANET. Using these approaches, we can prevent unauthorized nodes from joining in the network. They will give a significant overhead for verification and key exchange with the limited intrusion elimination. Apart from this, prevention-based techniques are less helpful to cope with malicious insiders who possess the legitimate credentials to communicate in the network.

Numerous IDSs for MANET have been recently introduced. Because of the nature of MANET, most of the IDS are structured to be distributed and have a cooperative architecture. Similar to signature based and anomaly based IDS models for the wired network and for MANET use statistics-based or specification-based approaches. Approaches like Specification-based, DEMEM [14] and [15], [16], [17], monitor network activities and compare them with the features of known attacks that is not practical to cope with unknown attacks. But the statistics-based approaches, like Watchdog [18], and [19], compare network activities with normal behavior patterns, that will leed to higher false positives rate than the specification-based ones. Due to already available false positives in MANET IDS models, intrusion alerts from these systems comes with alert confidence, which will indicates the probability of attack occurrence.

When it comes to make response decisions [20], there always exists inherent uncertainty which leads to unpredictable risk, particularly in security and intelligence arena. To tackle this problem, Risk-aware approaches are introduced by balancing action benefits and damage trade-offs in a quantified way

VI CONCLUSION

In this project, a more efficient method of detecting replica attacks is proposed. Replica nodes have all valid credentials so, they are able to easily launch an attack in a MANET undetected. These attacks can range from passive attacks like traffic monitoring, eavesdropping, etc. to active attacks like blackhole attack, flooding, location disclosure attack, spoofing attack, etc.

Here, the network parameters have been optimized by the efficient detection of replica nodes. Here detection schemes like Time Domain Detection Scheme and Space Domain Detection Scheme are used. Also a protocol called Location

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

Information Exchange Protocol is also used for efficient replica attack.

REFERENCES

[1] Y. Sun, W. Yu, Z. Han, and K. Liu, "*Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks*," - IEEE J. Selected Areas in Comm., VOL. 24, No. 2, pp. 305-317, Feb. 2006.
[2] M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, "*Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks*," - IEEE Trans. Computers, VOL. 59, No. 5, pp. 707-719, May 2010.
[3] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, Ruoyu Wu, "*Risk Aware Mitigation For MANET Routing Attacks*" - IEEE Trans. On Dependable and secure Computation, VOL.9, No.2, March/April 2012.
[4] L. Sun, R. Srivastava, and T. Mock, "*An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions*," - J. Management Information Systems, VOL. 22, No. 4, pp. 109-142, 2006.
[5] C. Mu, X. Li, H. Huang, and S. Tian, "*Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory*," - Proc. 13thEuropean Symp. Research in Computer Security (ESORICS '08),pp. 35-48, 2008.
[6] K. Sentz and S. Ferson, "*Combination of Evidence in Dempster- Shafer Theory*," technical report, Sandia Nat'l Laboratories, 2002.
[7] L. Zadeh, "*Review of a Mathematical Theory of Evidence*," AI Magazine, vol. 5, no. 3, p. 81, 1984.
[8] R. Yager, "*On the Dempster-Shafer Framework and New Combination Rules*[*]*1*," Information Sciences, vol. 41, no. 2, pp. 93- 137, 1987.
[9] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "*Sensor Fusion Using Dempster-Shafer Theory*," Proc. IEEE Instrumentation and Measurement Technology Conf., vol. 1, pp. 7-12, 2002.
[10] T. Clausen and P. Jacquet, "*Optimized Link State Routing Protocol*," Network Working Group, 2003. vol. 11, no. 1, pp. 21-38, 2005.
[11] B. Levine, C. Shields, and E. Belding-Royer, "*A Secure Routing Protocol for Ad Hoc Networks*," Proc. 10th IEEE Int'l Conf. Network Protocols (ICNP '02), pp. 78-88, 2002.
[12] Y. Hu, D. Johnson, and A. Perrig, "*SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks*," Ad Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.
[13] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "*ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks*," ACM Trans.
[14] Information and System Security, vol. 10, no. 4, pp. 1-35, 2008.
[15] C. Tseng, S. Wang, C. Ko, and K. Levitt, "*DEMEM: Distributed Evidence-Driven Message Exchange Intrusion Detection Model for Manet*," Proc. Ninth Int'l Symp. Recent Advances in Intrusion Detection (RAID '06), pp. 249-271, 2006.
[16] C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt, "*A Specification-Based Intrusion Detection Model for OLSR*," Proc. Ninth Int'l Symp. Recent Advances in Intrusion Detection (RAID '06), pp. 330-350, 2006.
[17] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, "*Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET*," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan./Feb. 2011.
[18] J. Felix, C. Joseph, B.-S. Lee, A. Das, and B. Seet, "*Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA*," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 2, pp. 233-245, Mar./Apr. 2011.
[19] S. Marti, T. Giuli, K. Lai, and M. Baker, "*Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*," Proc. ACM MobiCom, pp. 255-265, 2000.
[20] S. Kurosawa, H. Nakayama, N. Kato, and A. Jamalipour, "*Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method*," Int'l J. Network Security, vol. 105, no. 627, pp. 65-68, 2006.
[21] T. Toth and C. Kruegel, "*Evaluating the Impact of Automated Intrusion Response Mechanisms*," Proc. 18th Ann. Computer Security Applications Conf. (ACSAC '02), pp. 9-13, 2002.

BIOGRAPHY

Dr.P.GaneshKumar received B.E (EEE) from Madurai Kamaraj University in 2001 and M.E(CSE) with distinction from Bharathiar University in 2002. He received PhD degree in information and communication engineering in 2011 from Anna University Chennai. He also received MBA degree form Madurai Kamaraj University in 2009.

He has 10 years of teaching experience in Information Technology. Currently he is working as Professor in department of IT at PSNA College of Engineering and Technology. He is a member of IEEE, life member of ISTE and life member of CSI. He had published 21 papers in international journal, 6 papers in IEEE international conference and 25 papers in national conference.

He authored two books called Component Based Technology and Fundamentals of pervasive computing. He is member in advisory committee and technical committee for various national and international conferences. He is also reviewer for number of International Journals, International and National conferences. He had delivered guest lectures in various colleges and universities on several topics. His area of interest includes distributed systems, computer network, ad hoc network and cryptography & network security.

Mr.K.RajKumar received B.E (CSE) from Madurai Kamaraj University in 2004 and M.E(CSE) from Anna University in 2007. Currently he is pursuing Ph.D from Anna University Chennai.

He has 7 years of teaching experience in the departments of Computer Science and Engineering and Information Technology. Currently he is working as Associate professor in department of IT at PSNA College of Engineering and Technology. He is a life member of ISTE. His area of interest includes computer Network, Network Programming & Management and Data Structures.

Mr.P.Senthilkumar received B.E (CSE) from Raja College of Engineering in 2002 and M.Tech(CSE) from SRM Engineering college in 2005. He has 8 years of teaching experience in the departments of Computer Science engineering and Information Technology. Currently he is working as Associate professor in department of IT at PSNA College of Engineering and Technology.. His area of interest is wireless Networks.