ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

Enhancing Security in MANET using Integral Component Cluster-Based Certificate Revocation with Vindication Capability

[1]S.Herman Jeeva, [2]K.Girija, [3]S.Bellze Mary, [4]D.Saravanan

[1,2,3] PG Scholar, Department of Computer Science and Engineering, Pavendar Bharathidasan college of Engineering and Technology, Tiruchirapalli, Tamilnadu, India.

[4]Associate Professor. Department of Computer Science and Engineering, Pavendar Bharathidasan college of Engineering and Technology, Tiruchirapalli, Tamilnadu, India.

ABSTRACT - Mobile Adhoc Networks (MANETs) is the open network environment where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANETs is not secure than the wired networks. To overcome this problem, the Cluster-based Certificate Revocation is proposed with Vindication Capability (CCRVC) scheme. Each cluster consists of a Cluster Head along with some Cluster Members (CMs) located within the transmission range of their cluster Head. Before nodes join the network, they have to acquire valid certificates from the Certification Authority (CA) that is responsible for distribution and management of certificates to all nodes. The CA is also responsible of updating two lists, Warning list and Black list, which are used to hold the accusing and accused nodes information, respectively. Experimental results show that the proposed scheme is effective and efficient to provide secure communication.

KEYWORDS - Mobile ad hoc networks (MANETs), certificate revocation and security.

I. INTRODUCTION

In MANETs, certificate management is the mechanism that is widely used since it helps in delivering trust in a public key infrastructure [12], to protect applications and network services. For certificate management, a complete security solution has three components such as prevention, detection, and revocation. Many research efforts took place in some areas such as certificate distribution [14], attack detection [2], [6] and certificate revocation [1]. In order to secure network communications, Certification is essential. The public key is encrypted into an attribute using the digital signature of the issuer. It is used to assure that a public key belongs to an individual and helps in preventing tampering and forging in mobile Adhoc networks.

Enormous research efforts are made to abate malicious attacks on the network. If any attack is identified, Certificate revocation plays a major task of enlisting and removing the certificates of nodes which have been detected to launch attacks on the neighborhood. This helps in removing misbehaving nodes from the network and gets blocked from all its activities suddenly. Certificate revocation's basic security problem is aimed at providing secure communications in MANETs.

This paper proposes a Cluster-based Certificate Revocation with the scheme of Vindication Capability (CCRVC) which has ability to enhance the performance of MANET. Topology is constructed as clusters. A cluster consists of nodes within the transmission range and each cluster has Cluster Head (CH) and Cluster Member (CM). The nodes having a valid certificate alone are allowed to join the network. Certification Authority (CA) issues the valid certificates. Nodes are arranged as clusters that ensures preloading of certificate which is responsible for distributing and managing certificates of all nodes which in turn can communicate with each other without any constraints. The CA updates two lists such as Warned list and Black lists that holds information of accusing and accused nodes respectively.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

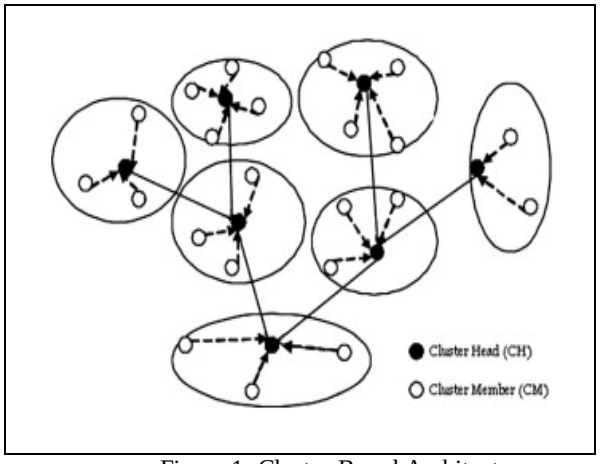

Figure 1: Cluster-Based Architecture

Voting-based mechanism is the one which cancels (revokes) a malicious attacker's certificate through votes from valid neighboring nodes. Neighboring nodes issues certificates for new joining nodes. Based on votes from its neighbors, the certificate of an attacker is revoked. In URSA, each nodes helps in performing one-hop monitoring and exchange their monitoring information with their neighboring nodes. The certificate of the accused node is revoked when the number of negative votes exceeds a predetermined value.

Since nodes cannot communicate with others without a valid certificate, certificate revocation of a voted node leads to the isolation of that node from network activities. Threshold determination remains a challenge. If it exceeds the network degree, nodes that are launching attacks cannot be cancelled or revoked and can communicate with other nodes successively.

False accusations which are malicious are not addressed by URSA from nodes is a critical issue. Arboit et al. [1] proposes the scheme which allows all nodes that are connected in the network to vote together. In URSA, no Certification Authority (CA) exists in the network, but each node plays a role of monitoring the behavior of its neighbors. The primary difference from URSA is that nodes vote with different weights. Node's weight is calculated in terms of reliability and trustworthiness of the node which is derived from its past behaviors that can be the number of accusations against other nodes and that against itself from others. The stronger its reliability, the acquired weight is increased. When the weighted sum from voters against the node exceeds a predefined threshold, the certificate of an accused node is normally revoked. This improves the accuracy of certificate revocation. However, the communications overhead used to exchange voting information would be high and it increases the revocation time because all nodes are required to participate in each voting.

A given node deemed as a malicious attacker will be decided by any node with a valid certificate in the non-voting-based mechanism. The scheme of Clulow et al. [4] proposed a fully distributed "suicide for the common good" strategy, in which only one accusation completes certificate revocation quickly. Simultaneously, certificates of both the accused node and accusing node have to be revoked. To remove an attacker from the network, the accusing node has to sacrifice itself. Although this approach reduces both the time required to evict a node and communications overhead of the certificate revocation procedure due to its suicidal strategy, the application of this strategy is limited. Furthermore, this suicidal approach does not take into account to differentiate falsely accused nodes from genuine malicious attackers.

As a consequence, the accuracy is reduced. A cluster-based certificate revocation scheme, where nodes are self-organized to form clusters was proposed by Park et al. [10]. In this scheme, control messages are managed by a trusted certification authority, holding the accuser and accused node in the warning list (WL) and blacklist (BL), respectively. Any single neighboring node can revoke the certificate of the malicious attacker node. Further, it also deals with the issue of false accusation that enables cluster head (CH) to remove the falsely accused node from the blacklist. The process of handling the certificate revocation is completed in short time.

The high accuracy in confirming the given accused node as a real malicious attacker or not is the main advantage of the voting-based mechanism.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

The disadvantages are slow decision process to satisfy the condition of certificate revocation and also it incurs heavy communications overhead to exchange the accusation information for each other. On the contrary, a suspicious misbehaved node can be revoked by only one accusation from any single node with valid certification in the network in the non-voting-based method.

The decision-making process for rapid certificate revocation can be simplified and also reduce the communications overhead. However, determining the accuracy of an accused node as a malicious attacker and the reliability of certificate revocation will be reduced as compared with the voting-based method. This performance emphasize the difference between voting-based method which achieves higher accuracy in judging a suspicious node, but takes a longer time and the non-voting-based methods can significantly expedite the revocation process.

Vindication Capability (CCRVC) scheme is proposed for Cluster-based Certificate Revocation [10], [8]. In this, clustering is incorporated in the proposed scheme, where the cluster head plays an important role in detecting the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation.

CCRVC achieves prompt revocation and lowering overhead as compared to the voting-based scheme and improves the reliability and accuracy as compared to the non-voting-based scheme.

II. THE PROBLEM

It is difficult to identify the attackers through wireless Adhoc network since it is a self configured network. Various revocation techniques are used for enhancing network security. Voting based mechanism and non-voting mechanism are two types of mechanisms for certificate revocation,

Voting based mechanism

In URSA, one-hop monitoring is performed and monitoring information is exchanged with its neighboring nodes by each node. A predefined number is maintained as a threshold for getting negative votes by each node. The certificate of accused node gets revoked when the number of negative votes for a node exceeds the threshold value.

Then, the node can get isolated from the network activities. However, the accused node would be communicating with other nodes in network when threshold value is assigned larger. The risk factor is that false accusation from malicious node is not addressed.

Arboit et al.[15] proposed that voting varies with the weights. Based on reliability and trustworthiness which can be derived from its past behaviors, the weight of a node is calculated. The certificate can be revoked when the weighted sum from voters against the node exceeds a predefined threshold. The accuracy of certificate revocation can be improved and communication overhead would be high when all nodes are participated in each voting.

Non-voting based mechanism

Certificate revocation can be quickly completed by only one accusation in “suicide for the common good” strategy i.e., both the accused node and accusing node certificates will be revoked simultaneously. In this, the time required to evict a node and communications overhead of the certificate revocation procedure can be reduced. But there is degradation in accuracy.

III. CONTRIBUTION

Cluster-based Certificate Revocation is proposed with Vindication Capability (CCRVC) scheme. In this, the cluster head plays an important role in detecting the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation.

CCRVC achieves prompt revocation and lowering overhead as compared to the voting-based scheme and improves the reliability and accuracy as compared to the non-voting-based scheme. Attacker nodes are revoked by Cluster-based revocation scheme upon receiving only one accusation from a neighboring node.

In order to guard against malicious nodes from further framing other legitimate nodes, the scheme maintains two types of lists called warning list and blacklist. Moreover, false accusation can be addressed by the cluster head to revive the falsely revoked nodes by adopting the clustering architecture. In this, the focus is on the certificate revocation procedures once a malicious attacker has been identified, rather than the attack detection mechanism itself. Each node has the ability to detect its neighboring attack nodes which are within one-hop away.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

Clusters are formed with cooperation of nodes and each cluster consists of a CH with some Cluster Members (CMs) located within the transmission range of their CH. Nodes have to acquire valid certificates from the CA before they join the network, which is responsible for distributing and managing certificates of all nodes, so that nodes can communicate with each other.

Nodes propagates a CH Hello Packet (CHP) to notify neighboring nodes periodically when it proclaims itself as a CH,. The nodes within the transmission range of CH can accept the packet to participate in this cluster as cluster members.

Nodes are classified as normal node, warned node, and revoked node based on their reliability

Normal Node: It is a node that joins the network and does not launch attacks. It has high reliability which has the capacity to accuse other nodes and to declare itself as a CH or a CM.

Warned Node: Nodes in the warning list are regarded as warned nodes with low reliability. They are considered suspicious because the warning list contains a mixture of legitimate nodes and a few malicious nodes.

Revoked Node: The accused nodes that are listed in the blacklist are called as revoked nodes with little reliability. They are considered as malicious attackers deprived of their certificates and evicted from the network.

IV. SYSTEM DESIGN

The system design involves the different steps involved in the proposed Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. The entire process is summarized in the Fig.2 which gives a clear cut idea about the proposed method.

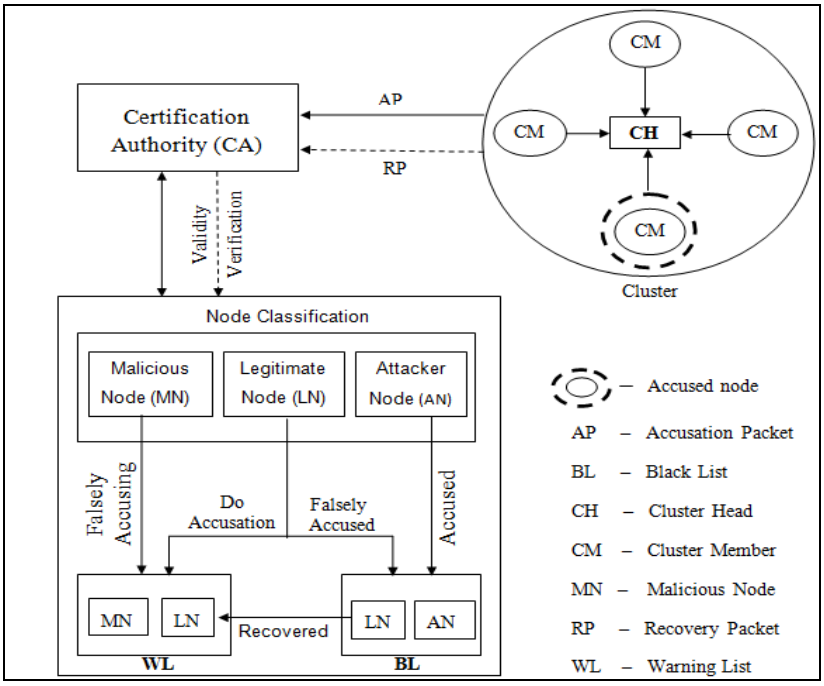

Figure 2: System Architecture for CCRVC Scheme

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

Process:

When the neighboring nodes detect attacks from any one node then each of the nodes sends out an accusation packet to the certificate authority (CA) against attacker node. According to the first received packet, the CA holds neighboring node and attacker node in the Warning List (WL) and Black List (BL)., respectively, after verifying the validity of neighboring node the CA disseminates the revocation message to all nodes in the network. After receiving the revocation message nodes update their local WL and BL to revoke attacker's certificate. Meanwhile, CH update their WL and BL and determine that one of the node was framed. Then some of the nodes send recovery packet to the CA to revive the falsely accused node. Upon receiving the first recovery packet, the CA removes the falsely accused node from the BL and holds both the falsely accused node and normal node in the WL and then disseminates the information to all the nodes. At last the nodes update their WL and BL to recover the falsely accused node.

V. SYSTEM IMPLEMENTATION

Simulation of AODV Protocol

Creation of nodes and transmission of packets between those nodes is made by Normal Network with AODV protocol. The calculation of parameters such as end to end delay, throughput, packet delivery ratio, energy spent is done.

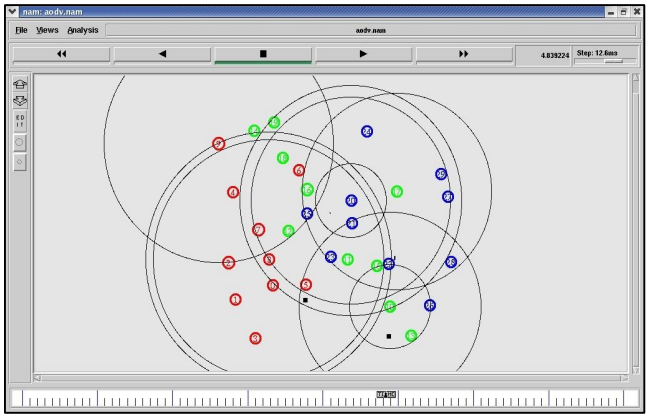

Figure 3: Creation of nodes and Transmission of packets using AODV protocol

Simulation of DoS Attack

Implementation of DoS Attack during packet transmission makes the performance degradation. The parameters such as end to end delay, throughput, packet delivery ratio, energy spent are calculated.

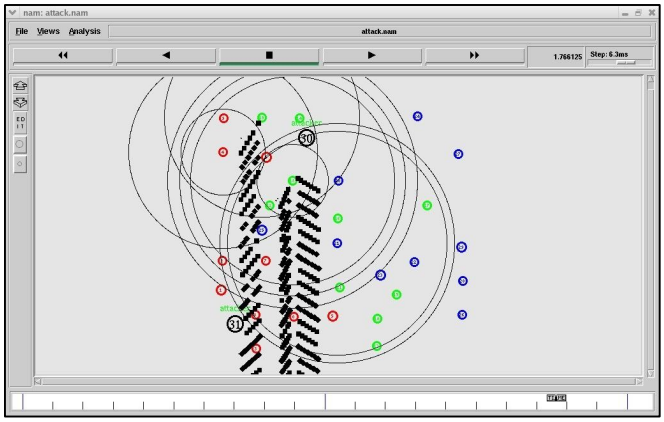

Figure 4: Dropping of packets

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

Simulation of CCRVC Scheme

Using proposed Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme, transmission of packets between the nodes is done to avoid attack and to increase network performance. The Calculation of parameters such as end to end delay, throughput, packet delivery ratio, energy spent is made.

VI. PERFORMANCE EVALUATION

Comparison between AODV, ATTACK and CCRVC with various parameters is done and output is shown using graph.

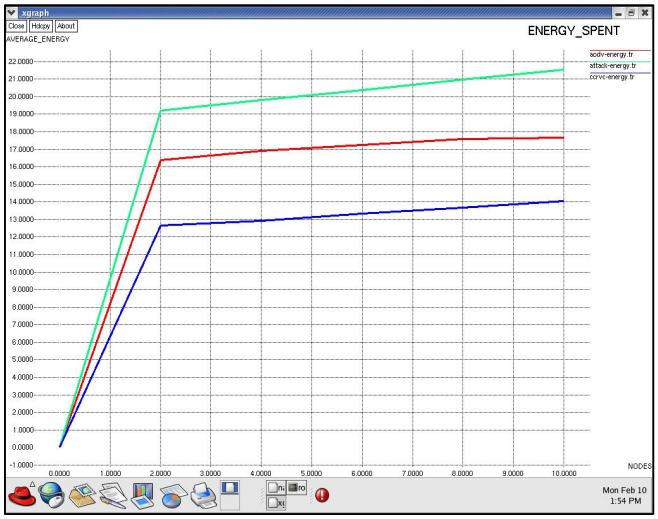

Figure 5: Graph Representing Variations of Energy

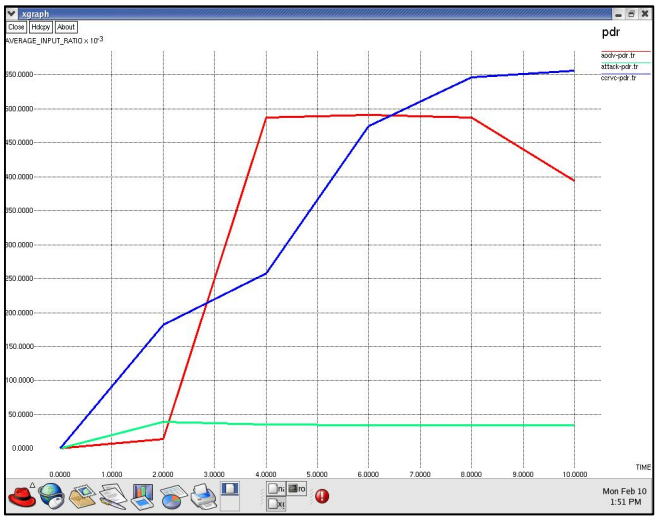

Figure 6: Graph Representing Variations of Packet Delivery Ratio

All the above graphs show the variation of delay, energy, packet delivery ratio and throughput with respect to time.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

VII.CONCLUSION AND FUTURE ENHANCEMENT

A major issue, certificate revocation of attacker nodes is addressed, which in turn ensures a secure communications in MANET. Cluster-based certificate revocation with vindication capability scheme has merits of both voting-based and non-voting based mechanisms in which malicious certificate is revoked and false accusation problems are solved. This scheme reduces the revocation time as compared to the voting-based mechanism. In addition, falsely accused nodes are restored by the CH in the cluster based model easily, which improves the accuracy as compared to the non-voting based Mechanism. The legitimate nodes are released and restored in a new incentive method which also improves the number of available normal nodes in the network for ensuring the efficiency of quick revocation. Thus the scheme of CCRVC is more effective and efficient in certificate revocation of malicious attacker nodes, reducing revocation time, and improving the accuracy and reliability of certificate revocation.

REFERENCES

[1] Arboit G., Crepeau C., Davis C.R. and Maheswaran M. "A Localized Certificate Revocation Scheme for Mobile Adhoc Networks," Adhoc Network, vol. 6, no. 1, pp. 17-31, 2008.

[2] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato. "A survey of routing attacks in mobile Adhoc networks", 2007.

[3] Camp T., Boleng J. and Davies. "The survey of mobility models for Adhoc network research," Wireless Communication and Mobile Computing, vol.2, no. 5, pp. 483-502, 2002.

[4] Clulow J. and Moore T. "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems," ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, 2006.

[5] Hegland A.M., Winjum E., Rong C. and Spilling P. "A survey of key management in Adhoc networks," IEEE Communications Surveys and Tutorials, vol 8, no. 3, pp. 48-66, 2006.

[6] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto and Nei Kato. "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Adhoc Networks", 2009.

[7] Jie Lian, Kshirasagar Naik, Gordon B. and Agnew. "A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks", 2004.

[8] Liu W., Nishiyama H., Ansari N. and Kato N. "A Study on Certificate Revocation in Mobile Adhoc Network," Proc. IEEE Int'l Conf. Comm. (ICC), 2011.

[9] Luo J., Kong P., Zerfos S., Lu and Zhang L. "URSA: Ubiquitous and Robust Access Control for Mobile Adhoc Networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063, 2004.

[10] Park K., Nishiyama H., Ansari N. and Kato N. "Certificate Revocation Cope with False Accusations in Mobile Adhoc Networks," Proc. IEEE 71st Vehicular Technology Conf. (VTC '2010).

[11] Sakarindr P. and Ansari N. "Security services in group communications over wireless infrastructure, mobile Adhoc, and wireless sensor networks," IEEE Wireless Communications, 14(5), 2007.

[12] Yang H., Luo H., Ye F., Lu S. and Zhang L. "Security in mobile adhoc networks: challenges and solutions," IEEE Wireless Communications,11(1), pp. 38-47, 2004.

[13] Yang H., Shu J., Meng X. and Lu S. "SCAN: Self-Organized Network-Layer Security in Mobile AdHoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 261-273, 2006.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

[14] Zhou L., Cchneider B. and Van Renesse R. "COCA: A Secure Distributed Online Certification Authority," ACM Transactions on Computer Systems, Vol.20, No.4, pp.329-368, 2002.

[15] Zhou L. and Haas Z. J. "Securing Adhoc networks," IEEE Network Magazine, 13 (6), pp. 24-30, 1999.

BIOGRAPHY

Mr. HERMAN JEEVA S received the B.E degree in Computer Science and Engineering from St.Joseph's College of Engineering and Technology, Thanjavur in 2012. He is currently doing his M.E in the same stream in Pavendar Bharathidasan College of Engineering and Technology, Mathur, Tiruchirappalli.

Ms. GIRIJA K received the B.E degree in Computer Science from SKP Engineering College, Tiruvannamalai in 2012. She is currently doing her M.E in the same stream in Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli.

Mrs. BELLZE MARY S received the B.E degree in Computer Science from Pavendar Bharathidasan College of Engineering and Technology, Tiruchirapalli in 2004. She is currently doing her M.E in the same stream in Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli

Mr. SARAVANAN D received the B.E degree in Electrical and Electronics Engineering from Maharaja Engineering College, Tiruppur in 2000 and received the M.E degree in Computer Science and Engineering from Annamalai University, Chidambaram in 2005. He is currently doing the Ph.D. in the area of MANET and also working as an Associate Professor in Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli with 11 years of teaching experience and his area of interest include MANET.