An Effective Reliable Secure Data Gathering and Intrusion Detection Scheme for WSN

S. Gopinath, N. A. Natraj, N. Suresh Kumar

Abstract*: *Wireless Sensor Network is a indivisible part of network where it has no infrastructure. In the past, Intrusion detection systems were used to detect intrusions in network effectively. Most of the systems are able to detect intrusions with high false alarm rate. In this paper, we propose a Effective Trust based Intrusion Detection System (ETIDS) for detecting malicious activities and providing authentication as well as data integrity. To achieve this, Cluster based routing is established based on trust vector of neighbor nodes in random topology. Trust based Recommendation and key based authentication protocol is integrated with clock based verification method to identify malicious nodes. Simulation results shows that the ETIDS provides better detection efficiency, packet delivery ratio, low end to end delay, successful certification rate and low overhead than existing schemes.

Index Terms*: *WSN, Intrusion Detection System, Data Gathering, Malicious, Mobility, packet delivery ratio, Detection efficiency and delay.

I. INTRODUCTION

A. Wireless Sensor Network

Wireless Sensor Networks (WSNs) are composed of detector nodes and sinks. Detector or Sensor nodes have the aptitude of self healing and self-organizing. Nodes are localized and distributed in nature wherever communication takes place via multi-hop intermediate nodes. The most objective of a detector node is to gather information from its encompassing surroundings and transmit it to the sink. WSNs have several applications and are employed in situations like detective work temperature change, observance environments and habitats, and numerous alternative police investigation and military applications. Primary detector nodes are employed in such areas wherever wired networks are not possible to be deployed. WSNs are deployed in physical harsh and hostile environments wherever nodes are invariably exposed to physical security risks damages. Moreover, self-organizing nature, low battery power provide, restricted information measure support, distributed operations victimization open wireless medium, multi-hop traffic forwarding, and dependency on alternative nodes are such characteristics of detector networks that expose it to several security attacks in the slightest degree layers of the OSI model.

Revised Manuscript Received on 15 November 2018.

Dr. S. Gopinath, Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore (Tamil Nadu), India,

Prof. N. A. Natraj, Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India.

Dr. N. Suresh Kumar, Department of Electronics and Communication Engineering, AVS Engineering College, Salem, India.

WSNs are susceptible to many sorts of security attacks because of open wireless medium, multi-hop localized communication, and preparation in hostile and physically non-protected areas. Totally different threat models are mentioned in mote-class attacks and laptop-class attacks. In mote-class attacks, the assailant compromises few of the detector nodes within a WSN. In laptop-class attacks, the assailant have additional powerful devices to launch additional intense attack against WSNs. Security attacks against WSNs is classified as active and passive. Passive attacks are silent in nature and are conducted to extract necessary info from the network. Passive attacks don't damage the network or network resources. Active attacks are usually to do misdirect, temper, or drop packets. The distinctive characteristics like wireless medium, contention-based medium access, multi-hop nature, localized design, and random preparation of such networks create them additional susceptible to security attacks at different layers.

II. RELATED WORK

Kannan and Sree Renga Raja [1] introduced cluster head scheduling algorithm to provide maximum network lifetime in WNS. Based on signal strength, the election of CH was done for both primary and secondary tier networks. Residual energy and Signal strength decides the selection of CH and to avoid frequent selection of CH in order to satisfy the distribution of cluster heads. In each cluster, all dedicated and superior nodes are called as CH. The scheduling algorithm was used to support network density and to provide high efficiency.

Shivkumar et.al [2] proposed robust and energy efficient single mobile destination based data gathering protocol based on expectation maximization concept. During the formation of cluster, the following issues are identified i.e. number of cluster heads, cluster nodes, cluster density, path capability and transmission range. In presence of expectation concept, the energy wastage is dramatically reduced using cluster count estimation technique. The energy efficiency and data gathering ration are improved based on the selection of paths and estimation of transmission accuracy.

Sarmad Rashed and Mujdat Soyturk [3] analyzed the UAV mobility patterns. Mobility pattern plays a major role that follows various paths to provide best coverage in a least amount of time. A new metric is introduced to provide tradeoff between minimum execution time and coverage region during the selection of suitable mobility pattern. A novel simulation pattern is used to compare the parameters of the system.

The effects of clustering and mobility patterns are analyzed to maximize the covered node ratio with the use of clustering algorithms.

Weimin Wen et.al [4] analyzed from the previous strategies and proposed the efficient data collection scheme with maximum energy efficiency among sensor nodes. The path may be increased from the selection of visiting sensor nodes. Due to more time consuming, sensor buffer overflow may be arisen. In this research work, authors proposed data collection scheme to choose set of sensor nodes based on rendezvous points (RPs). The efficient paths for mobile destination are chosen to collect data based on the RPs. If any sensor nodes are not visited by destination node, the readings will be forwarded to nearest RPs to improve data collection efficiency.

Alhasanat et.al [5] proposed new data gathering technique with mobile elements. It is referred to as Intersectioon Point of Communication Ranges. Whenever the reduction of data collection latency occurs, the optimal trajectory of mobile sink will be computed by means of intersection points. Compared to connectivity based data collection algorithm, this algorithm achieved less data gathering latency and high network throughput.

Shilip Mahajan et.al [6] introduced the new strategy for cluster head election based on QoS. In this strategy, the concept of cluster chain weight metrics is adopted to improve the network performance. The major concerns in this strategy are formation of clusters with balanced routing and selection of suitable CHs. Initially, CHs are selected in the network based on weight metric and formation of clusters will begin. The energy is conserved among all sensor nodes and load is balanced. In addition to this, local clustering algorithm is also integrated to reduce communication cost and computation cost. Range based metric approach is adopted to choose clusters and distributes the load in the clusters and minimum energy is consumed.

Mohamed Benaddy et.al [7] developed a new multipath routing algorithm with energy consumption constraints for reliable transmission of packets. Based on energy conservation and distance between the nodes, reliability is estimated in the multipath routes. In this multipath algorithm, each node is assigned with a weight to provide reliable data packet transmission through reliable paths. Based on weight, a node can identify nearby neithbor node to transmit the packets in the network.

Gopi and Thirumurugan et.al [8] introduced the energy-efficient LEACH Protocol based on cluster routing. The data gathering efficiency is improved by selecting reliable CH and adopting low energy clustering hierarchy with adaptive routing. The gaussian model is adopted for node deployment based on mobility pattern. While forming a cluster, mobility of node plays a major role. Information from one node to another node is forward based on the energy efficient routing strategy.

Vinotha and Senthil Kumar [9] developed an efficient data gathering approach based on new sink relocation method. According to remaining energy of nodes, the transmission range of each sensor node is adjusted by incorporating the energy aware transmission range concept. If energy is getting low after message transmission and environmental defects, the transmission range is tuned to minimum for energy saving. The base routing protocol is maximum capacity based to prolong the network lifetime.

Sliha buyukcoraky et.al [10] introduced the localization method based on maximum likelihood concept for gamma shadow fading method to improve data collection accuracy and categorize the channel conditions. The received signal strength measurement is adopted to validate the model for indoor environment. The effectiveness of the proposed scheme is investigated to ensure data collection from source to destination.

Dhatchayani and Kannan [11] presented agent based data gathering scheme based on destination nodes. The concept of virtual binary-tree infrastructure based data gathering scheme is adopted to find the status of destination location. The data is collected based on the movement of destination node in left and right leaf areas inside the network region..After the end of data collection, the breaking time is estimated and broadcast overhead is reduced.

Ez-Zaidi Asmaa and Rakrak Said [12] proposed a new data collection scheme based on mobility pattern to decrease the latency and improve the staying time between destination nodes. If any data is to be delivered quickly, the information will be reached without delay. Data gathering process is affected due to high mobility of destination nodes and short communication between destination node and sensor nodes. Only a small amount of data packets will be delivered to destination nodes due to high speed.

Mariam Alnuaimia et.al [13] introduced data collection based on ferries. It eliminates the need for multi-hop forwarding of data to reduce the maximum energy consumption. But the packet delivery latency is increased and it is not suitable for all kind of applications. Based on effect of ferry's path, data collection is done. The CH is chosen based on distance from ferry path and residual energy. The decision of choosing CH is based on remaining energy of nodes and replacing of CHs using energy threshold technique. Data is gathered by ferry instead of multi-hop routing.

Rumpa Dasgupta and Seokhoon Yoon [14] developed the energy efficient deadline aware data gathering scheme using mobile data collectors. These collectors gather information from all sensors and send it to CH. It also recharges the sensor nodes using the wireless power transfer technology. Due to the presence of data collectors, energy consumption is reduced and packet delay constraint is satisfied to find an optimal path.

Chao Wu et.al [15] proposed a data gathering scheme based on path of destination nodes and communication range of nodes inside the cluster region. In the graph based data gathering scheme, the network region is estimated and algorithm complexity is greatly reduced. The sensor node inside the grid is moved within location. This scheme produced maximum delivery rate and less latency while attaining high network density.

III. PROPOSED INTRUSION DETECTION SYSTEM

A. Intrusion Detection Algorithm

In this phase, proposed protocol consists of three modules. In the first module, cluster based secure multicast routing is established from one cluster to another cluster based on security challenges. In WSN, major challenges are data confidentiality, authentication, and data availability. In second module, packets are distributed through multicast routes to achieve global connectivity. The data transmission scheme is introduced to make network more secure with the help of data encryption and decryption algorithm. In third module, data gathering is achieved based on secure network routing procedure. The proposed protocol contains the following assumptions.

- Cluster region is formed by identifying cluster members within transmission region and cluster head is chosen based on transmission energy.
- Secure transmission routes are established from CH to cluster members. Each route contains trust vectors to find any malfunction in the paths and links.
- Data transmission is implemented with confidentiality using asymmetric key distribution scheme.
- Data gathering is achieved in network with network routing procedure.

B. Cluster based Secure Multicast Routing for Data Gathering

In this module, cluster is formed based on transmission distance, network capacity, link capacity and node stability. Node stability is a major concern in cluster formation where nodes are moving with high mobility. Residual energy of a node is estimated before cluster formation. Nodes are actively participated in data transmission. After certain period, residual energy will be estimated. Links are fluctuated during packet transmission. Cluster is formed once all nodes are inside the region and within transmission distance. CH is selected based on maximum residual energy and high stability. Stability of a node is estimated based on packet delivery rate with less packet loss. There are two phases in cluster routing i.e route request phase and route reply phase.

In route request phase, the routes are established and updated to form a multicast group from CH to cluster members. In other case, CH forms a multicast group with the collection of receivers. The receivers are identified with minimum hop count. CH initiates the route request phase by flooding a *Join Multicast Request Group (JMRG).* The contents of JMRG are *Sequence Number (SN), Multicast Address (MA), CH Address (CHA), Time to Live (TTL), Stability Factor (SF), Hop Count (HC) and Multicast Route Request ID (MRRID).* Once the original JMRG packet is received at neighbor nodes, it will respond via *Joint Route Reply (JRR)* packets.

In route reply phase, the collection of destination nodes or receivers or cluster members receives the packets and responds via JRR packets which contains the source CH sequence number, hop count and received stability factor. The stability factor lies between 0 and 1 which is generated by cluster members. Cluster members CM_1, CM_2 *and* CM_3 receive JMRG packets and verify its authenticity by validating its signatures. After verification, *CM* creates the entry of multicast routing towards CH. If any malicious activities

The subject determines the trust values of objects according to both straight and circuitous trust values. Assume the node *k* is subject, which not only makes straight assessment of object l, but also makes circuitous estimation of object l through nodes k_1, k_2 and k_3 . It is assumed that node k makes trust estimation for node l and adopted acknowledgement mechanism. In this case, trust threshold value is maintained to find the malicious node. If any node falls below the trust threshold value, it is considered as misbehaving node. The trust threshold value includes packet arrival rate, packet sending rate, packet forwarding rate, reliability factor, node recommendation and node proposal. The determination of the above packets is given below.

Step 1: Compute the packet arrival ratio based on acknowledgement packets to total packets available in the link.

Step 2: Determine the packet sending rate based on the computation of different time slots and packet loss rate.

Step 3: Source forwards the packets including UPDATE packet to know the status of forwarding capacity of links and neighbor nodes.

Step 4: Compute the reliability factor based on mobility and stability of nodes. If a node with stable link is predicted, packets will be reliable based on stable neighbor nodes.

Step 5: Compute the threshold from packet forwarding, packet arrival and packet sending rate. The threshold value is fixed to 82 based on node mobility and link stability. If any node goes below the threshold value, it is considered as malicious node.

IV. PERFORMANCE EVALUATION

A. Simulation Model and Parameters

The attacks withstand by proposed system are cipher text attacks, Denial of Service attacks, Replay attack, Worm hole attack etc. In previous work, all these attackers are not solved perfectly. The proposed IDS is simulated with Network Simulator tool (NS 2.34).

Table 1. Experimental Setup of ETIDS

No. of Nodes	200
Area Size	1200 X 1200 m^2
Mac	802.15.4
Radio Range	250m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	80 bytes
Protocol	E-LEACH

B. Performance Metrics

The following parameters are used to check the performance of proposed scheme.

Detection Efficiency: The ratio of identified malicious nodes to total number of nodes available in the zone.

Average end-to-end delay: The delay occurs from source to destination based on packet transmission and propagation.

Average Packet Delivery Ratio: It means that number of packets received to sent packets.

Communication Overhead: It defines that number of excessive packets to average packets.

Packet Integrity Rate: It defines that the ratio of number of genuine packets to duplicate packets.

C. Results

Figure 2 show the results of detection efficiency for the nodes 10, 20, 30….100 scenarios. Clearly our scheme achieves more detection rate (35.34 – 97.88)% than the previous schemes. Because of cluster based routing. In this routing, link stability is maintained and malicious nodes are identified using the trust recommendation and clock based certificate determination. Therefore the vulnerability of malicious nodes is reduced.

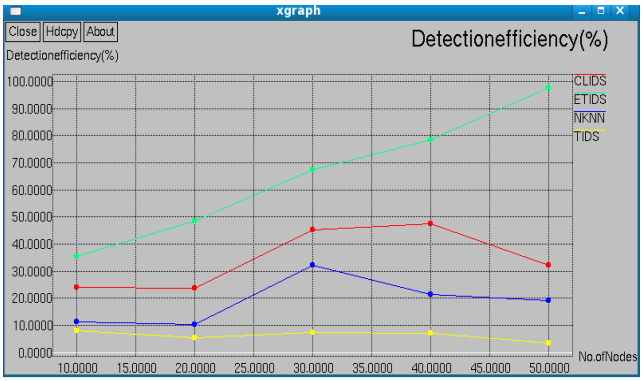

Figure 2. No. of Nodes Vs Detection Efficiency

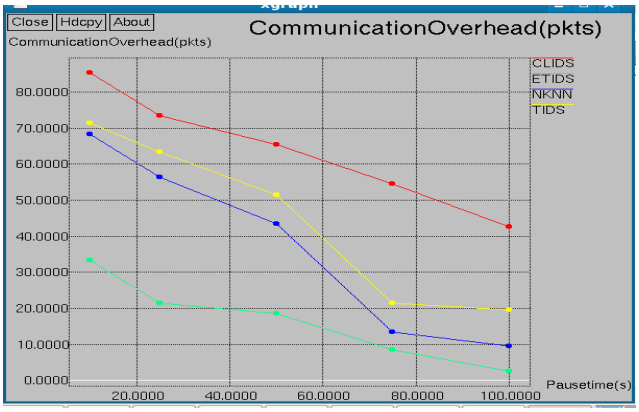

Figure 3. Pause time Vs Communication Overhead

Figure 3 shows the results of Pause time Vs Communication overhead. From the results, we can see that proposed IDS achieves less overhead (33-0.02) packets than previous schemes. It is because of link stability determination. Cluster head chooses only high stable link for data forwarding. So the network delivery rate is getting increased. Packet overhead will be suppressed because of link quality and reliability of neighbor nodes.

Figure 4 shows the results of packet delivery ratio for the speed. Clearly our system achieves more packet delivery ratio (98.7- 95.8)% than previous intrusion detection systems. The proposed system comprises two major aspects i.e. malicious detection and network authentication. Packet is delivered via reliable nodes through stable link. Successfully all the packets are delivered to the destination.

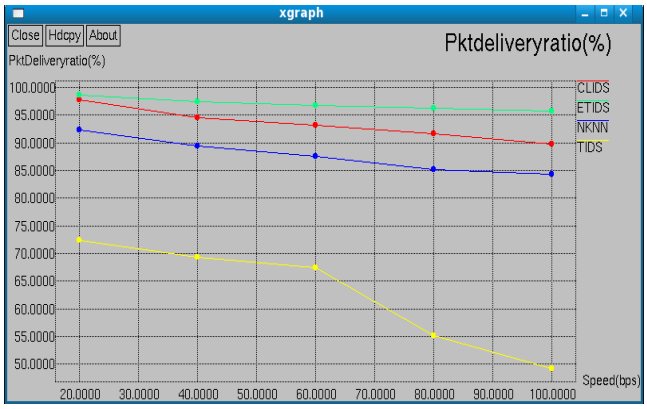

Figure 4. Speed Vs Packet Delivery Ratio

Figure 5 shows the results of Mobility Vs end to end delay. From the results, we can see that proposed system has less delay (0.2-0.04)ms than previous systems. End to end delay should be kept minimum in order to satisfy QoS. The proposed system reduces delay by means of cluster based routing. Network partitioning will be reduced by integrating this routing in all networks.

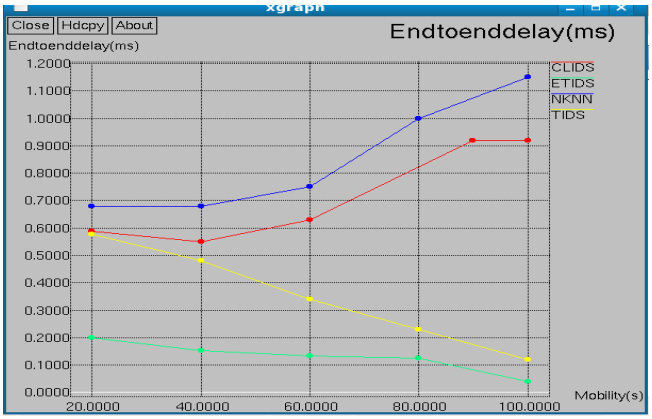

Figure 5. Mobility Vs End to end delay

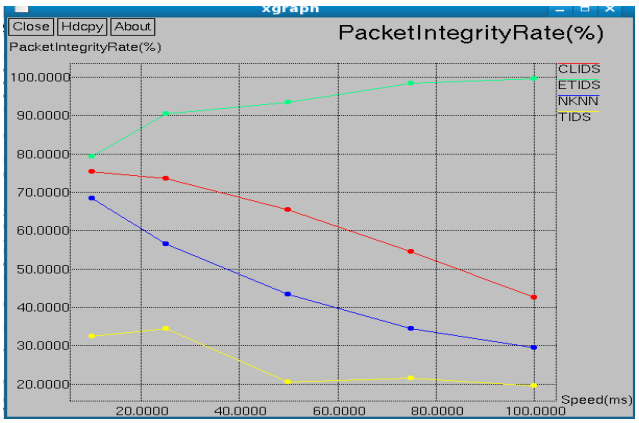

Figure 6. Speed Vs Packet Integrity Rate

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Figure 6 shows the results of Speed Vs Packet Integrity Rate. From the results, we can see that proposed system has high integrity (79 - 99) % than previous systems. The proposed system increases network packets integrity based on encryption and decryption scheme performance. Table 2 presents the performance comparison of proposed and existing schemes.

V. CONCLUSION

In WSN, it is easy to deploy the malicious attackers during packet transmission phase. These attacks modify the packet information, drop the packets and misroute the packets to wrong destination. If it continues, network partitioning may likely to occur and it leads to network dis-connectivity. To avoid this, several intrusion detection systems were proposed to identify malicious attackers with less false positive rate. In this proposed scheme, an effective intrusion based secure intrusion detection system is designed to make balance between intrusion and authentication status. Based on the simulation results, the proposed scheme achieves better performance than existing schemes in terms of performance metrics.

In future work, we have planned to include fuzzy decision tree with supervised clustering which will be implemented to classify the data sets and node in terms of selfish behavior. Selfish behavior nodes grasp the information for its purpose only.

REFERENCES

1. T G. Kannan and T. Sree Renga Raja, "Energy efficient distributed cluster head scheduling scheme for two tiered wireless sensor network", Egyptian Informatics Journal, Vol.16, 2015, pp.167–174.
2. Shivkumar S. Jawaligi, G. S. Biradar, " Single Mobile Sink Based Energy Efficiency and Fast Data Gathering Protocol for Wireless Sensor Networks", Wireless Sensor Network, 2017, Vol.9, pp.117-144.
3. Sarmad Rashed and Mujdat Soyturk, "Analyzing the Effects of UAV Mobility Patterns on Data Collection in Wireless Sensor Networks", Sensors, Vol.413,2017, pp.1-21.
4. Wenjun Liu, Jianxi Fan, Shukui Zhang, Xi Wang, "Relay Hop Constrained Rendezvous Algorithm for Mobile Data Gathering in Wireless Sensor Networks", Springer, Lecture Notes in Computer Science, LNCS-8147, pp.332-343, 2013,
5. Ching-Hsien Hsu; Xiaoming Li; Xuanhua Shi; Ran Zheng. 10th International Conference on Network and Parallel Computing (NPC), Sep 2013, Guiyang, China.
6. Alhasanat, K. Alhasanat and M. Ahmed, "Range based data gathering algorithm with a mobile sink in Wireless Sensor Networks", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 7, No. 6, December 2015, pp.1-13.
7. Shilpa Mahajan , Jyoteesh Malhotra , Sandeep Sharma, "An energy balanced QoS based cluster head selection strategy for WSN", Egyptian Informatics Journal, Vol.14, 2014, pp.189-199.
8. Mohamed Benaddy*, Brhim El Habil, Othmane El Meslouhi, Salah-ddine. Krit, "A Mutlipath Routing Algorithm for Wireless Sensor Networks Under Distance and Energy Consumption Constraints for Reliable Data Transmission", International Journal of Sensors and Sensor Networks, 2017, Vol.5, No.5-1, pp.32-35.
9. Gopi Saminathan Arumugam and Thirumurugan Ponnuchamy, "EE-LEACH: development of energy-efficient LEACH Protocol for data gathering in WSN", EURASIP Journal on Wireless Communications and Networking, 2015, Vol.76, pp.1-9.
10. Vinotha and Senthil Kumar, " An Effectual Data Gathering Approach Using Sink Repositioning For WSN", SSRG International Journal of Electronics and Communication Engineering, 2017, pp.146-153.
11. Saliha Büyükçoraky, Günes Karabulut Kurt, Abbas Yongaçoglu, "An Empirical Study on Gamma Shadow Fading Based Localization", European Signal Processing Conference, 2017, pp.2778-2782.
12. C.Dhatchayani and S.Kannan, "Agent Based Efficient Data Gathering Scheme for Wireless Sensor Networks with a Mobile Sink", International Journal of Emerging Technology in Computer Science & Electronics, Vol.24, Issue 4, 2017, pp.10-15.
13. Ez-Zaidi Asmaa and RAKRAK Said, "Mobility for an Optimal Data Collection in Wireless Sensor Networks", International Journal of Advanced Computer Science and Applications, Vol. 8, No.7, 2017, pp.353-360.
14. Mariam Alnuaimi, Khaled Shuaib, Klaithem Alnuaimi and Mohammed Abdel-Hafez, "Ferry-Based Data Gathering in Wireless Sensor Networks with Path Selection", The 6th International Conference on Ambient Systems, Networks and Technologies, 2015, Vol.52, pp.286-293.
15. Rumpa Dasgupta and Seokhoon Yoon, "Energy-Efficient Deadline-Aware Data-Gathering Scheme Using Multiple Mobile Data Collectors", Sensors, 2017, pp.1-23.
16. Chao Wu, Yuan'an Liu, Fan Wu, Wenhao Fan and Bihua Tang, "Graph-Based Data Gathering Scheme in WSNs With a Mobility-Constrained Mobile Sink", Special Section on Emerging Trends, Issues, and Challenges in Energy-Efficient Cloud Computing, IEEE Access, Vol.5, 2017, pp.19463-19477.

Authors Profile

Dr. S. Gopinath is working as Associate Professor in Department of ECE at Karpagam Institute of Technology, Coimbatore. He has completed his UG B.E. Electronics and Communication Engineering at Government College of Engineering, Salem in 2007 and PG M.E. Communication Systems in Anna University of Technology, Coimbatore in 2011. He earned his PhD in the field of Information and Communication Engineering at Anna University, Chennai in 2016. He was worked as Software Developer – Front end designer in Mahindra Satyam Services Ltd during 2007-2009. He has 5 Scopus journals and two SCI index journals and 12 peer reviewed journals to his credit. His research area is Ad-hoc and Sensor Networks.

N.A. Natraj is currently working as Assistant Professor in ECE Dept. at Prince Shri Venkateshwara Padmavathy Engineering College, Chennai. He is pursuing his Ph. D at Karpagam University. He completed his M.E in Anna University, Coimbatore and B.Tech ECE in SATRA University. His research interests include Communication Networking in Wireless sensor networks. He has 7 years of teaching experience in various countries. His publication has 3 Scopus indexed journals and 12 International Journals.

Dr. N. Sureshkumar is working as Associate Professor in Department of ECE at AVS Engineering College, Salem. He completed his UG B.E. Electrical and Electronics Engineering at Mohammed Sathak Engineering College in 2001and M.E. Applied Electronics in KSR College of Technology in 2005. He earned his PhD in the field of Communication Engineering at Karpagam Academy of Higher Education in 2018. He has 3 Scopus journals and one SCI index journal and 4 peer reviewed journals to his credit. His research area is Wireless Communication and Networking.