International Journal of Scientific Research in Multidisciplinary Studies
Vol.4, Issue.9, pp.38-43, September (2018)

Survey Paper
E-ISSN: 2454-9312
P-ISSN: 2454-6143

A Survey On Defending Against Cooperative Jamming Attacks In Internet of Things

E. Selvi[1*], K. Renuka[2]

[1]Research scholar, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India
[2]HoD & Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India

**Corresponding Author: selvipoet@gmail.com*

Available online at: www.isroset.org

Received: 12/Sept/2018, Accepted: 20/Sept/2018, Online: 30/Sept/2018

***Abstract*—** Jamming attacks are a subset of denial of service (DoS) attacks in which malicious nodes block legitimate communication by causing intentional interference in networks. Jamming represents the most serious security threat in the field. Security abides a tremendous key requirement in the context of Internet of Things (IoT). IoT connects multiple objects together through wired and wireless connections in the aim of enabling ubiquitous interaction where any components can communicate with each other without any constraint. One of the most important elements in the IoT concept is IOT. In this survey paper of all the security issues in the field of IoT along with the analysis of the various architecture of IoT. The study defines various security actions, its requirements and the challenges that come along with the implementation of IoT. Finally, a number of techniques and problem future work is presented to enhance IoT security (Privacy, Lightweight crypto, etc.).

***Keywords*—** Jamming Attack, Internet of Things, denial of service, Wireless Sensor Networks, Security

I. INTRODUCTION

Nowadays, billions of people are active using Internet for all kinds of purposes on a daily basis. People send in fact emails, use social networks, share voice and image, transfer money, watch events, and perform many more actions with it. It is estimated that by 2020, there will be 50 to 100 billion devices connected to Interne. If what is happening now was difficult to conceive 20 years ago, one can easily imagine that future will be as unpredictable, if not even more.

IoT is a system that provides connectivity and interactive communication to anything. Although the term "being connected" is commonly used in electronic devices in day to day life, physical objects (i.e. hardware's) such as actuators, sensors, etc. are connected with single address of the internet protocol. The wires connection or the wireless connection of the network data is consciously transmitted through the hardware to interpret. Because of the property to communicate and sense physical objects can understand the complications of the surroundings and react. These physical objects have been set up and accepted extensively and they are working appropriately without the involvement of humans. In near future, it is estimated that every day to day object will be a part of Internet. Mobile phones and similar devices will act as remote control to objects in the world and usually called as IoT. According to Gartner, the number of devices that are connected to internet is expected to rise from 25 billion to 50 billion near 2020. The rising popularity of the network leads to new risks of security and the attackers can take even more private information of the users/organizations which are associated with that IoT system. The main purpose of this thesis is to highlight the security concerns in IoT environment.

Wireless sensor networks (WSNs) form the major part of the IoT. They are used in many fields such as health, agriculture, environment and detection of natural disasters. The fundamental characteristics of WSN make it vulnerable to attacks due to the operating nature of its components (wireless broadcasting). This will exhibit them to passive and active attacks, which vary by nature and goals. Wireless communications are exposed to eavesdropping and signal interception. One such attack that can occur almost in all environments is radio jamming.

MAC protocols are vulnerable to intelligent jamming attacks. Some of the existing protocols fail to deliver any packet in the case that they are being exposed to a jammer. In case of large-scale networks with high-energy constraints, nodes are

scheduled to communicate and sleep simultaneously as in TDMA-based protocols. The aim is to avoid overhearing and idle listening that represent the major sources of energy loss. However, such a temporal ordering can introduce a pattern of communication that allows the attacker to predict the next communication cycle. This can be exploited by a malicious node to launch an energy-efficient attack. Accordingly, jammed signals coincide with the packets sent from legitimate network nodes. The malicious node will be able to exploit the temporal pattern of communication and block sending legitimate packets with a small set of jamming pulses. Therefore, it achieves the same energy-efficiency as network nodes and becomes more difficult to spot.

Jamming attacks may be viewed as a special case of Denial of Service (DoS) attacks. Wood and Stankovic define DoS attack as "any event that diminishes or eliminates a network's capacity to perform its expected function". Typically, DoS prevents or inhibits the normal use or management of communications through flooding a network with 'useless' information. In a jamming attack the Radio Frequency (RF) signal emitted by the jammer corresponds to the 'useless' information received by all sensor nodes. This signal can be white noise or any signal that resembles network traffic.

Jamming in wireless networks is defined as the disruption of existing wireless communications by decreasing the signal-to-noise ratio at receiver sides through the transmission of interfering wireless signals. Jamming is different from regular network interferences because it describes the deliberate use of wireless signals in an attempt to disrupt communications whereas interference refer to unintentional forms of disruptions. Unintentional interference may be caused by the wireless communications among nodes within the same networks or other devices (e.g. microwave and remote controller). On the other hand, intentional interference is usually conducted by an attacker who intends to interrupt or prevent communications in networks. Jamming can be done at different levels, from hindering transmission to distorting packets in legitimate communications.

The organization of this paper is as follows: Section 2 describes the overview of different type of jamming attacks. In Section 3, we give the details existing jamming attack detection algorithms. Section 4 conclude of work.

II. OVERVIEW OF JAMMER

Jamming makes use of intentional radio interferences to harm wireless communications by keeping communicating medium busy, causing a transmitter to back-off whenever it senses busy wireless medium, or corrupted signal received at receivers. Jamming mostly targets attacks at the physical layer but sometimes cross-layer attacks are possible too. In this section, we elaborate on various types of jammers and the placement of jammers to maximize the jammed area. There is different type of jamming attack.

A. Types of jammers

Jammers are malicious wireless nodes planted by an attacker to cause intentional interference in a wireless network. Depending upon the attack strategy, a jammer can either have the same or different capabilities from legitimate nodes in the network which they are attacking. The jamming effect of a jammer depends on its radio transmitter power, location and influence on the network or the targeted node. A jammer may jam a network in various ways to make the jamming as effective as possible. Basically, a jammer can be either elementary or advanced depending upon its functionality. For the elementary jammers, we divided them into two sub-groups: proactive and reactive. The advanced ones are also classified into two sub-types: function-specific and smart-hybrid.

- Proactive jammer

Proactive jammer transmits jamming (interfering) signals whether or not there is data communication in a network. It sends packets or random bits on the channel it is operating on, putting all the others nodes on that channel in non-operating modes. However, it does not switch channels and operates on only one channel until its energy is exhausted.

- Reactive Jammer

Reactive jammer starts jamming only when it observes a network activity occurs on a certain channel. As a result, a reactive jammer targets on compromising the reception of a message. It can disrupt both small and large sized packets. Since it has to constantly monitor the network, reactive jammer is less energy efficient than random jammer. However, it is much more difficult to detect a reactive jammer than a proactive jammer because the packet delivery ratio (PDR) cannot be determined accurately in practice. According to the following are two different ways to implement a reactive jammer.

- Function-specific Jammers

Function-specific jamming is implemented by having a pre-determined function. In addition to being either proactive or reactive, they can either work on a single channel to conserve energy or jam multiple channels and maximize the jamming throughput irrespective of the energy usage. Even when the jammer is jamming a single channel at a time, they are not fixed to that channel and can change their channels according to their specific functionality.

- Smart-hybrid Jammers

The smart because of their power efficient and effective jamming nature. The main aim of these jammers is to

magnify their jamming effect in the network they intend to jam. Moreover, they also take care of themselves by conserving their energy. They place sufficient energy in the right place so as to hinder the communication bandwidth for the entire network or a major part of the network, in very large networks. Each of this type of jammer can be implemented as both proactive and reactive, hence hybrid.

B. Placement of jammers

The attacker possessing the above qualities, placement of the jammer plays an important role in effective jamming. Jammers can be placed randomly or can be placed based on a jamming technique which locates the best position to accomplish its objective of jamming with as many nodes as possible. In this section, we will inspect this optimization problem by looking at various placements of jammers.

- Optimal jamming attacks

The probability of jamming can be made high if the attacker is aware of the network-strategy as well as its transmission powers. In addition, the jammer needs to have knowledge about the network channel access probabilities and the number of neighbors to the monitor node (detecting node). All the other nodes in the network just perform the usual IEEE 802.11 simplex communication. The monitor node uses the Sequential Probability Ratio Test for sequential testing between two hypotheses concerning probability of false alarm and probability of missed detection.

- Jamming under complete uncertainty

A dynamic approach to compute the location for placing jamming devices by integrating the bounds of the area to be jammed. They assume a square-shaped area encloses the network where the jammers are placed at the intersections of a uniform grid. They formulate the problem as follows. If the jammers have to optimally jam all the nodes of the network then where should they be placed. Sub-problems are created and solved in order to achieve an optimal result.

- Limited-range jamming attacks

Jammers with transmission range half that of legitimate nodes can jam the network because the interference range of wireless devices is twice the transmission range. Contrary to the above schemes this jamming attack does not require global knowledge. Besides, due to the limited transmission range, these jammers are not easily detected. These jammers are placed at strategic locations. Usually the locations are close to the nodes which have the maximum traffic flow (in/out). The authors have shown the experimental results using normal range, limited range and double range (transmission range) jammers.

- DSS for locating VHF/UHF jammer

A jamming system which should be placed at the optimum location such that it completely demolishes the communication capability of the target system. These kinds of systems are usually used by military applications. More number of candidate points or selected points for deploying jammer system is considered in comparison to the target points and the number of jamming systems available. They assume there is line-of-sight between the jammer and target systems, targets are within the antenna range, and the signal power of the jamming system is higher than the signal power of the target system.

- Nano size jammer

The use of a large number of tiny, low-power jammers that are difficult to detect as they are not visible to the naked eye, being so smaller in size. The implementation of these jammers is in the form of a network. With the total jamming power being constant, they achieve a phase transition of jamming throughput. Reactive jammers are deployed throughout the network. Researchers discussed the traditional literature on jamming primarily focusing on the design of physical layer technologies, such as spread spectrum, that are resistant to Radio Frequency (RF) jamming. It should be realized that the physical layer technologies needed to reliably resist jamming have not found widespread deployment in commodity wireless devices, such as wireless LANs and sensor networks.

III. RELATED WORK

With the widespread deployment of WSNs, jamming attacks that send malicious radio signals to disrupt legitimate communication and consume resources, and its countermeasures have been studied in the literature. This is necessary as sensor nodes are vulnerable to this type of attack due to their architecture, hostile deployment and insecure routing protocols.

A greedy user can increase his share of bandwidth by slightly modifying the driver of his network adapter. The greedy user may try to corrupt the Request to Send (RTS) and Clear to Send (CTS) of other users to prevent packet transmission, or may corrupt ACKs to cause the ACK contention window to increase, leading to larger back off. They proposed DOMINO, a system that has to be implemented only at the AP for detection of such greedy behaviour in the MAC layer of IEEE 802.11 public networks. DOMINO algorithm is conducted by collecting the traffic traces and run several tests on them.

T.X. Brown et., al., [1] This paper presented initial results in designing such a layered attacker for the Transport/Network layer. Jamming can get significant jamming gains, well over 100, when it knows the packet type and timing. Interestingly most of these gains were produced by attacking packets above the ad hoc network layer. Protocols introduce highly predictable timing that can be exploited. The limited

information of packet size, timing, and sequence is enough to accurately predict packet types. A. Chan et., al., [2] introduce a novel T-resilient scheme that requires at most $(Tlog_T N)^2$ control information retransmission to guarantee the delivery of such information to all users against any coalition of T traitors. The proposed scheme also allows the identification of the traitors. Our next step is to extend the combinatorial method for the multiple traitor case. It will be interesting to investigate the scheme which assigns different number of keys to different users and analyse its performance.

W. Xu et., al., [3] in this paper proposed the creation of a jamming-resistant timing channel to restore the availability of communication links in the presence of interference. The timing channel is built as a low-rate physical layer overlay on top of the traditional physical/link-layers. Our timing channel uses the detection and timing of failed packet receptions at the receiver, which we have shown is possible by time stamping CRC failures or by monitoring the signal strength. P. Tague at., al., [4] in this approach the problem of designing control channel access schemes which allow for efficient reception of control messages while maintaining a degree of independence between the hopping sequences held by different users. In this work, we focus our attention on designing schemes which are robust to control channel jamming attacks by malicious colluding insiders or compromised users.

Alnifie G et., al., [5] This paper presents MULEPRO (Multichannel Exfiltration Protocol), a fully distributed network-based protocol designed to rapidly exfiltrate data from a jammed area. MULEPRO targets sensor network applications that require an immediate and robust response to radio jamming denial-of-service (DoS) attacks. It works by automatically and efficiently assigning nodes to different channels in the jammed area in order to defeat an attacker. Alnifie G et., al., [6] MULEPRO (Multi-channel Exfiltration Protocol), a fully distributed network-based protocol designed to rapidly exfiltrate data from a jammed area using multiple communication channels simultaneously. The basic idea is to assign scheduling symbols to the different nodes based on their vertex color to produce conflict-free transmission schedules between sensor nodes, up to two-hop distance in order to address the terminal hidden problem. MULEPRO targets sensor network applications that require an immediate and robust response to such jamming-based DoS attacks and is designed to operate with any number of channels. When an attack is launched nodes can effectively coordinate exfiltration transmissions without needing to exchange network protocol information.

A jamming attack commences, jammed nodes and their boundary neighbors operate by switching into exfiltration mode. Each jammed node attempts to send out data packets multiple times using different channels in such a way as to ensure that the attacker cannot attack all nodes. For commodity level sensor radios the challenge is to schedule when nodes are sending and when they are receiving, while at the same time attempting to utilize as fully as possible all available channels. Further, it is highly desirable to avoid all two-hop wireless collisions arising from one or two-hop neighbors using the same channel at the same time. MULEPRO solves these problems using a vertex-coloring approach followed by a distributed scheduling technique based on Latin squares.

Bellardo J et., al., [7] The 802.11-based wireless access networks has led to widespread deployment in the consumer, industrial and military sectors. However, this use is predicated on an implicit assumption of confidentiality and availability. While the security flaws in 802.11's basic confidentially mechanisms have been widely publicized, the threats to network availability are far less widely appreciated. In fact, it has been suggested that 802.11 is highly susceptible to malicious denial-of-service (DoS) attacks targeting its management and media access protocols. This paper provides an experimental analysis of such 802.11-specific attacks – their practicality, their efficacy and potential low-overhead implementation changes to mitigate the underlying vulnerabilities.

802.11-based networks have seen widespread deployment across many fields, mainly due to the physical conveniences of radio-based communication. This deployment, however, was predicated in part on the user expectation of confidentiality and availability. This paper addressed the availability aspect of that equation. We examined the 802.11 MAC layer and identified a number of vulnerabilities that could be exploited to deny service to legitimate users. We described software infrastructure for generating arbitrary 802.11 frames using commodity hardware and then used this platform to implement versions of the de-authentication and virtual carrier sense attacks. Chiang JT et., al., [7] in this paper code tree system that provides input to the physical layer and helps the physical layer circumvent jammers. In our system, the transmitter has more information than any proper subset of receivers. Each receiver cooperates with the transmitter to detect any jamming that affects that receiver. In the resulting system, each benign user is guaranteed to eliminate the impact of the attacker after some finite number of losses with arbitrarily high probability.

To adopt our protocol, a CDMA system must be able to assign each user a different set of spreading codes that should change over time. Most current CDMA systems already require a client registration phase, where each client is given an identification number. For example, a client needs to provide some identification in order to obtain 3G service on a CDMA phone with a unique electronic serial number (ESN). The set of spreading codes can thus be distributed during the registration phase. The use of time-varying spreading code is

not necessary for running our protocol; however, our protocol adopts time-varying spreading codes in order to prevent attackers from learning a spreading code by correlating messages over time. Our protocol does not require regular feedback from receivers; however, our broadcast transmitter does need to be able to receive jamming report from receivers occasionally.

Gencer C et., al., [9] In the study, a deployment model is suggested for the purpose of performing single (point jamming) or sequential frequency jamming on the VHF/UHF frequency band, for ground-based radio jammer systems operating as per principles of line-of-sight (LOS) warfare accepting a fixed antenna beam width. A decision support system (DSS) based on the suggested model has been created so as to enable us to present to the user's various alternatives related to deployment for different values of program parameters and to address different scenario conditions. Gummadi R et., al., [10] impact on 802.11 networks of RF interference from devices such as Zigbee and cordless phones that increasingly crowd the 2.4GHz ISM band, and from devices such as wireless camera jammers and non-compliant 802.11 devices that seek to disrupt 802.11 operation. Our experiments show that commodity 802.11 equipment is surprisingly vulnerable to certain patterns of weak or narrow-band interference. This enables us to disrupt a link with an interfering signal whose power is 1000 times weaker than the victim's 802.11 signals, or to shut down a multiple AP, multiple channel managed network at a location with a single radio interferer. We identify several factors that lead to these vulnerabilities, ranging from MAC layer driver implementation strategies to PHY layer radio frequency implementation strategies.

Khattab S et., al., [11] In this paper, we introduce the problem of maximizing network goodput under jamming attacks through a combination of channel hopping and error-correction coding. We describe the solution space and investigate one point thereof, namely reactive defense against scanning attack. We develop a Markovian model of the reactive channel-hopping defense against the scanning jamming attack and validate it using simulation experiments. Our results suggest that an adaptive defense, based on our model, would improve the resiliency of multi-radio networks against jamming. This paper considers the problem of maximizing network goodput under jamming attacks in multi-radio networks by combining channel-hopping and error-correcting codes (ECC).

Liu H et., al., [12] Finally, we conducted experiments using MicaZ motes and performed extensive simulations under different network configurations, such as various network node densities and jammer's transmission ranges. Our experimental results validate the jamming models, and we found that the VFIL approach is more effective under the widely-adopted region-based model than the more realistic SNR-based model. Further, simulation results show that our virtual force iterative approach is less sensitive to node densities and can achieve higher localization accuracy compared with centroid-based approaches. In this paper, we explored the task of diagnosing jamming attacks. In particular, we focused on localizing the jammer after a jamming attack is identified. We formulated the jamming effects in two jamming models, region-based and signal-to-noise-ratio (SNR)-based. The region-based model applies the free space propagation model to the received jamming signal power, whereas the SNR-based model utilizes the signal-to-noise-ratio at the receiver to better capture the effects of the jammer. Further, we categorized the network nodes into three states under jamming: JAMMED, BOUNDARY, and UNAFFECTED. By exploiting the state of each network node, we developed virtual-force iterative localization (VFIL) algorithm that utilizes the network topology to iteratively adjust the estimated location of a jammer until it reaches a close approximate of the true location. VFIL does not depend on the measuring signal strength inside the jammed region, and thus it is not affected by the disturbed network communication caused by jamming. VFIL has two variants: VFIL-Tr assumes the NLB of the jammer is known, whereas VFIL-NoTr needs to estimate the NLB of the jammer when estimating the jammer's location.

Misra S et., al., [13] the determinant metrics for jamming detection, and the existing methods of jamming detection as applied to the wireless sensor networks. We also discussed how our approach to the problem differed from the existing ones from three angles: (1) the scope of the lethality of the jammer being enlarged to include military jammers, (2) the existing approaches consider only two discreet levels of jamming, jammed and not jammed; where as we consider that decision about whether a node is jammed or not jammed is a fuzzy one and accordingly, aim to grade different node as per their jamming indices which suits the information war environment allowing various options to the war- zone commander (or, base station) in adopting different policies with respect to victimized nodes, and (3) the decision for jamming detection is taken by the nodes themselves in the existing methods, which we consider not feasible due to the resource constraints of the WSN nodes and their ineffectiveness in communicating with other nodes during jamming, and accordingly, we choose to do all processing and decision making at the base station on a holistic picture. Having done so, we then selected packets dropped per terminal (PDPT) and signal-to-noise ratio (SNR) as the input to our fuzzy inference system based on Mamdani model which gave the jamming index (JI) of various nodes as output.

Muraleedharan R et., al., [14] This paper proposed a novel method of avoiding sensor network under jamming attack by using evolutionary algorithm, the ant system. The

performance parameters such as hops, energy, distance, packet loss, SNR, BER and packet delivery influences the decision taken in anti-jamming techniques. The network under 75% ELINT jammer attack is shown to be functional indicating the robustness of the Ant system. The four scenarios presented in the result section reemphasize the fact that a sensor network remains functional and assesses the situation under all critical conditions. The sensor network considered in this paper is made simple with 16 nodes and ant agents. Mpitziopoulos A et., al., [15] In this article, we presented Hermes, a prototype node capable of performing frequency hopping along with DSSS to effectively defend jamming attacks. Our simulations have shown that Hermes nodes guarantee a satisfactory packet success delivery rate even in heavily jammed environments, as opposed to typical sensor nodes communication schemes.

IV. CONCLUSION

In this paper we discussed about IOT Sensor Networks technique and its problem. We also addressed the problem of selective jamming attacks under an internal threat model, where the hacker is a part of the network who is aware of network secrets and also the implementation details. Finally, in the future we anticipate that IOT, are designed with security in mind so that they didn't lack in security. As more secure IOT will be in the future, more possibilities and applications are sure to use IOTs. In this survey paper of all the security issues in the field of IoT along with the analysis of the various architecture of IoT.

REFERENCES

[1] T.X. Brown, J.E. James and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks", Proc. ACMInt'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.

[2] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors", Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.

[3] W. Xu, W. Trappe and Y. Zhang, "Anti-Jamming Timing Channels for Wireless Networks", Proc. ACM Conf. Wireless Network Security (WiSec), pp. 203-213, 2008.

[4] P. Tague, M. Li, and R. Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks", IEEE Trans. Mobile Computing, vol. 8, no. 9, pp. 1221-1234, Sept. 2009.

[5] Alnifie G, Simon R, "A multi-channel defense against jamming attacks in wireless sensor networks", In: Proceedings of the 3rd ACM Workshop on QoS and Security for Wireless and Mobile Networks, pp. 95–104, 2007.

[6] Alnifie G, Simon R, "MULEPRO: a multi- channel response to jamming attacks in wireless sensor networks", Wireless Communications and Mobile Computing 10(5):704–721, 2010

[7] Bellardo J, Savage S, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions", In: Proceedings of the 12th Conference on USENIX Security Symposium, pp. 15–28, 2003

[8] Chiang JT, Hu YC, "Cross-layer jamming detection and mitigation in wireless broadcast networks", IEEE/ACM Transactions on Networking 19(1):286– 298, 2011.

[9] Gencer C, Aydogan EK, Celik C, "A decision support system for locating VHF/UHF radio jammer systems on the terrain", Information Systems Frontiers 10(1):111–124, 2008

[10] Gummadi R, Wetherall D, Greenstein B, Seshan S, "Understanding and mitigating the impact of RF interference on 802.11 networks", In: Proceedings of the 2007 Conference on Applications, technologies, architectures, and protocols for computer communications, pp 385–396. 2007.

[11] Khattab S, Mosse D, Melhem R, "Modeling of the channel-hopping anti-jamming defense in multi-radio wireless networks", In: Proceedings of the 5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services, pp. 25:1–25:10, 2008

[12] Liu H, Liu Z, Chen Y, Xu W, "Determining the position of a jammer using a virtual-force iterative approach", Wireless Networks 17(2):531–547, 2011.

[13] Misra S, Singh R, Mohan SVR, "Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system", Sensors 10:3444–3479, 2010.

[14] Muraleedharan R, Osadciw LA, "Jamming attack detection and countermeasures in wireless sensor network using ant system", In: SPIE the International Society for Optical Engineering, vol 6248, p 62480, 2006.

[15] Mpitziopoulos A, Gavalas D, Pantziou G, Konstantopoulos C, "Defending wireless sensor networks from jamming attacks", In: IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, pp 1 –5, 2007.

AUTHOR'S BIOGRAPHY

Ms. E.SELVI has received her MSc degree in Software Systems from Sree Saraswathi Thyagaraja College, Pollachi affiliated Bharathiar University, Coimbatore, in 2011 and Pursuing M.Phil degree in Computer Science from Rathinam College of Arts and Science, Coimbatore affiliated Bharathiar University, Coimbatore. She is dedicated tamil poet from the last 10 years and published 5 tamil poem books with ISBN. She is currently writing naval book, name of "PAVAIYIN MAUNAM". She is won many prizes in both school and college level Poem, Debate and Essay competitions.

Mrs.K.RENUKA has received her MSc degree in Computer Science from Bharathiar University, Coimbatore, M.Phil degree in Computer Science from Madurai Kamaraj University and pursuing Ph.D degree in Computer Science from Rathinam College of Arts and Science, Coimbatore affiliated Bharathiar University, Coimbatore. She is dedicated to teaching field from the last 11 years and 2 years of industry Experience. She is interested in computer networks and wireless networks and 7 years of research experience. She is guided 7 M.Phil scholars and currently guiding 1 M.Phil scholar.

