International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Implementation of Wireless Sensor's Integration Possibilities and Attacks on Wireless Network Control

Poonkodi.R, N. SaravanaSelvam

Abstract*: Collection of independent sensor nodes is primarily used as a combination of wireless detection and data networks are called wireless sensor networks (WSN). Wireless networks face many unacceptable security threats as these types of sensors are used primarily in many critical tasks such as military applications, claims management, environmental conditions, health applications, and more. Although the energy problem of the sensor network is more critical due to the absence of sensor nodes. The suggestion that other classes of source-based attacks are referred to as vampire attacks. Vampire attacks result in greater use of power during message delivery, which in turn prevents the entire network from quickly emptying node batteries. Because it uses protocol complaint messages to create attacks that make it difficult to detect and prevent. In this article, we intend to study and analyze vampire attacks and their effects on WSN. We also study cryptographic techniques using solutions for these types of attacks. This document explores the investigation of vampire attacks and their solution is provided in combination with the Minimum Spanning Encryption (MST) and RC5 techniques.

Keywords: WSN Attacks; PLGP; Wireless Sensor Networks (WSN); MST; RC5;

I. INTRODUCTION

Wireless sensor networks are a type of Ad-Hoc network with a large collection of sensor nodes scattered over a wide area. It consists of a large number of nodes with limited energy and low computing power [1]. The WSN faces many practical challenges and theories that attract researchers. WSNs are used in many applications such as bandwidth reduction and delay tolerance. Applications range from public and military surveillance to environmental and health monitoring [2]. Sensor nodes can detect physical information, process raw information in combination with information capture, calculation, and wireless communication, and transmit it to the base station (BS) [2].

Manuscript published on November 30, 2019.
* Correspondence Author
Ms.Poonkodi.R*, Assistant Professor, Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, Tamilnadu, INDIA.
Email: poonkodi1905@gmail.com
Dr.N. SaravanaSelvam, Professor, Department of ECE, PSR Engineering College, Sevalpatti, Sivakasi.Tamilnadu, INDIA. Email: n.saravanaselvam@gmail.com

Trust point problem in wireless sensor network (WSN) has become more and more concentrated by now investigation. WSN security research is also advanced and has cryptographic mechanisms, intrusion detection systems, and production management protocols [1]. The basic goal of security in wireless sensor network (WSN) is to secure the system against various attacks such as base mixes, interceptions, node clones, and packet modifications and so on. [1]. Adequate battery life and memory make it impossible to build a network of sensors for traditional security devices. These types of network attacks are classified as routing attacks and data traffic attacks [2]. Attackers can easily inject malicious packets into the wireless medium. The biggest challenge for wireless sensor networks is developing energy efficient routing protocols for high power consumption [3].

Wireless Sensor Network (WSN) security is a very serious problem as sometimes the WSN is used in many critical activities. Some attacks on WSN security requirements, such as integrity, confidentiality, and data confidentiality. But what happens if the network is secure even when it is powerless or running on low power? Therefore, the WSN energy problem motivated me to focus on the energy drain attack. All attacks that damage the network, directly or indirectly, damage the energy of the network. But energy consumption is not their primary motive. Vampire attacks are energy-consuming attacks that focus primarily on the power consumption or network battery life. It cannot damage the net during an attack, but its effects are durable and unpredictable. Get clean power by injecting vampires.

Because WSN applications are primarily used for public or unmanaged areas, security issues are a fundamental challenge for these types of sensor applications. In the new security mechanism, references are made to PKI cryptography and symmetry key encryption and decryption. The challenge is to develop different types of WSN encryption techniques that can affect certain constraints such as memory capacity, power and processing.

A. Survey on attacks in WSN

Security vulnerabilities occur primarily in the form of communication details, unauthorized access to WSN, data changes with unauthorized access, and enhancements false data for unauthorized access. There are several violations described as follows:

Table 1 WSN Attack on Different Layers [3]

Layer	Attack
Application Layer	Data corruption , Repudiation
Transport Layer	SYN flooding, Session hijacking
Network Layer	Wormhole, location disclosure attacks, Blackhole, , Hello flooding, Resource consumption
Data link Layer	Traffic analysis and monitoring
Physical Layer	Eavesdropping, Jamming

The rest of the document is organized as follows: The introductory section of Part II of the vampire attack is described. Section III discusses various methods or techniques for detecting and preventing vampire attacks. Section IV examines the proposed scheme. Section V provides the analysis of the results. And in the last section, the document ends.

II. WSN ATTACK

As its name suggests, the WSN attack takes something on the network and something else is simply the power of the network. Therefore, it can also be called drainage attack. There have been many other sources of energy, but so far there has been less concern for damage. This attack does not damage the network by flooding the information system, but tries to transmit information in order to consume a lot of energy on the network [5]. It is an attack on the battery power consumption that can attack directly on the routing level protocol to block the network and use the node battery [3].

A. Classification

When detecting the source node path, find the shortest path using the shortest path routing protocol. The selected routes cannot be changed during the parcel delivery phase. In the process, the attack may have taken place. When malicious nodes are detected in the network, Adversary in the network generates a cycle that is one of the key issues in the network in which the power consumption of each network node increases.

The classification of vampire attacks is based on which the protocol is used when routing packets within the network. But there are two types of carousel attacks and other attack attacks.

Carousel Attack

Malicious nodes send packets with paths with a series of loops, so that the same node appears multiple times in the path. This type of attack is called carousel attack [6]. Fixing the carousel is shown in the figure. Sources send packages for drowning. Therefore, he must choose the path. As the picture of the optimal path shows, there is the source F-E-sink.

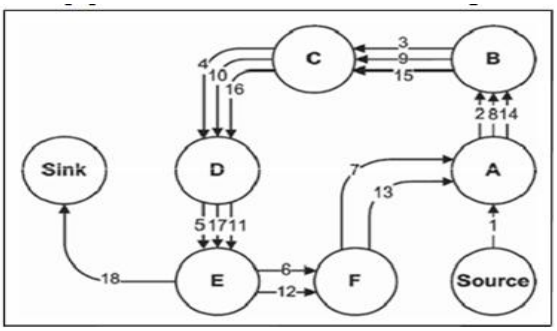

Fig. 1. Carousel Attack[12]

But the vampire insists on sending a packet to the A-B-C-D-E-sink source. The packet continues on this route 2-3 times, generating loops. Causes an electrical consumption of the network.

Stretch Attack

Malicious nodes develop an old false-packet path to reach a destination that moves the packet to a number greater than the ideal number of nodes for which this type of attack is called attack-by-extension [6]. Malicious stains are meant to generate the long path shown in the figure.

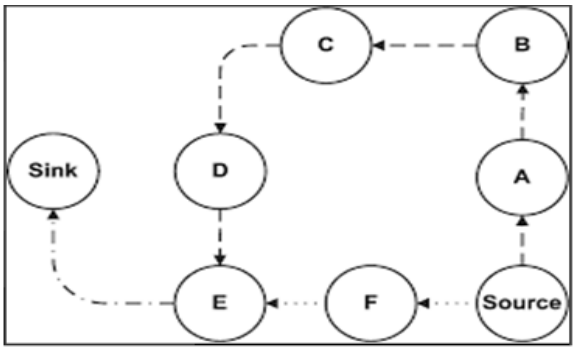

Fig. 2. Stretch Attack [12]

The optimal route for packets for the path from source to well is the F-E-sink source. But when a vampire provokes a stretch attack, this suggests a far-off source path-A-B-C-D-E-sink. Stretching attacks increase energy consumption by up to an order of magnitude, depending on the location of the damaged node.

B. Minimum Spanning Tree (MST)

The minimum range of points in an undirected oriented diagram is a low pass tree (among all scattered trees). It is a shed on a tree with an incorrect weight or equal to the weight of any tree that crosses it. The development of a single benefit involves the loss of property during the principal expulsion and the unilateral expulsion involves the loss of the net property. This is the shortest spread on the tree. The length of the tree is equal to the sum of the length of the curve on the tree.

C. RC5 Encryption

Cryptography calculation is a system or recipe that secures information or systems by providing security. Cryptography is a study of processing strategies for sending data into a secure structure so that the main subject is ready to extract that data as the intended recipient.

The use of excessive administrative systems encourages the exchange of information about the system when it is transferred to one or other of the managers. During the correspondence, he served as the basis for writing the message in order to prevent Gatecrasher from reading it. The security of the system is very cryptographic [18].

RC5 is a symmetrical master block code. RC remains for "Rivest Cipher" or otherwise known as "Ron Code". It is reasonable for the equipment and programming to work because they only use operations that are accessible on a normal chip [19]. The cryptographic calculation RC5 is a simple block of information about the contents of believers 16, 32 and 64 bits in a content block of the same length. The calculations are ordered in a set of cycles called r rounds accepting values. The RC5 works with two 32-bit A and B animators that contain the underlying information content or the normal content, as well as the performance numbers at the end of the encryption. We first compile the normal content in registers A and B, so that the cryptography and reorganization functions are linked to the latter [23].

III. RELATED SURVEY WORK

Wireless sensor networks are a huge area of research as they are sometimes used in some critical activities. Therefore, security issues need to be resolved or avoided. The main problem related to WSN is energy consumption. Since vampire attacks use energy, their effects, techniques and safety techniques are discussed in this review

Vasserman et al. [16] Vampire attacks are defined within Ad hoc wireless sensor network. Vampire attacks do not harm or divert existing routes, but use protocol complaint messages to damage the network. Observations of the safety measures and weaknesses of the existing protocols for vampire attacks are described. The proposed method, called PLGPa, can withstand attacks during certain phases of packet delivery. This is the first sensor routing protocol that can detect packet transfer to their destination node. Bhutada et al. [9] proposed the system in which it was used generate secure routes using the PLGP protocol and transfer data through topological routes. The proposed system performs four different tasks, namely secure path generation for data transfer, key management, attack node recognition and strip tracking techniques. Secure route generation is possible through the PLGP network routing / cleaning protocol, as vampire attacks cannot capture data transfer processes if they are implemented. In primary management, we use elliptical curve crystallography (ECC) based on the primary public cryptography method. on the structure of the elliptical curve. it shows that the result of PLGP is better than the BVR (Beacon Vector Routing) protocol.

Deshmukhet al. [8] proposed a new PLGP with validation (PLGPa) protocol indicating that the path history of each PLGP node should be used by PLGPa. Use the PLGP tree in which each node can go to its destination without interrupting the path. PLGPa is satisfied with its endless property. Each node sent must pass a validation string to confirm that the packet has not been moved from the destination node. An attacker can modify the fields so that he can only modify the authentication fields. Mariyappan et al. [6] presents a network protocol encryption protocol to maintain network availability. Use border recognition techniques to prevent vampires from attacking the ad hoc network. The proposed system has four main sections: Sensor Network Encryption Protocol (SNEP), Border Recognition Algorithm, Jump Point Algorithm, and Recursive Collection Algorithm. Tracks the network address routing table for each node. It incorporates a recursive grouping algorithm that verifies that each node in the network has a unique network address and routing table. The shortest and most accurate paths are generated without passing a node in less than 3 seconds using the jump point algorithm.

Abirami et al. [5] describes the Interior Gateway Routing Protocol (IGRP) and proposes a defense against several phases of delivery. IGRP is Cisco's proprietary remote telecommunication protocol, more scalable than Routing Information Protocol (RIP). The use of the PLGP IGRP limit can be solved. In PLGP, packages do not know which path is appropriate and which are harmful or have the right to make decisions regarding the choice of route. In the IGRP protocol, since it is a vector remote routing protocol, each packet has a routing table updated at regular intervals. As a result, some packages may make decisions about their discovery.

Ghate et al. [10] proposed the main authentication algorithm used by the group to prevent vampire attacks on wireless sensor networks. This algorithm has three main phases. The first phase is the pre-delivery master distribution level in which the network is divided into groups that have their own group ID. Each node in the network has provided its own public and private keys, public and private keys, and other public and private keys using elliptic curve cryptography (ECC).

Mittal et al. [33] proposed an attack; The enemy forces the beam to create a steering wheel before reaching its destination and a positive collision between the two enemies. When one of the enemies does NONACK, the other accomplice functions a bit like a legitimate knot and is called a resting point. To start with the enemy, the second will begin to circle before entering rest mode and, in this way, the second enemy will start one again before the break.

Deshmukh et al. [11] the authors proposed a defense against several attacks during the development phase and described the PLGPa. He is satisfied with the No-backtracking property

The packet is constantly heading towards its destination in the logical network address space and is being used against vampires. In the proposed system, each package keeps track of the same number of hops, whether or not the enemy is on the network. The PLGP packet is sent by the shortest path and does not respond to the nature of no backtracking.

IV. PROPOSED WORK

In WSN Attack, the attacker extends the package path or creates a loop. In both cases, the number of jumps will increase. As a result, we use a minimal spanning tree to limit route improvement. And so provide security with RC5 encryption techniques.

Step 1: All WSN nodes start the initialization process
Step 2: Run the neighbor discovery protocol
Step 3: Receive the initial information
Step 4: Select any starting node
Step 5: Select the node closest to the starting node to join the spanning tree.
Step 6: Select the closest node not presently in the Spanning tree.
Step 7: Repeat step 5 until all nodes have joined the Spanning tree.
Step 8: Spanning tree trims the path connections to avoid network loops
Step 9: RC5 Encryption is applied for better security purpose

V. SIMULATION PARAMETERS

Network Simulator Version 2 (NS-2) is a free and discrete event network simulator created by UC Berkeley. NS2 has evolved to become the most widely used open source network simulator and one of the most used network simulators. NS2 is composed of two main dialects: C ++ and OTL (Object-Oriented Device). Although C ++ describes the mechanism of incoming simulation objects (ie, the backend), OTcl provides the simulation by assembling and configuring objects and scheduling discrete events (i.e. The frontend). The simulation parameters are described as follows used to produce simulations for enemy models and proposed solutions.

Table 2. Simulation Parameters

Parameter	Values
Simulator	NS 2.3.4
Routing Protocol	AODV, MST
Scenario Size	1000 x 1000
Number of Nodes	50, 60, 70, 80, 90, 100
Simulation Time	100 sec
Traffic Type	Constant Bit Rate (CBR) / UDP
Packet Size	512 bytes
Packet Rate	4 packets/sec
Pause Time	5 sec
Maximum Speed	5, 10, 15, 20 m/sec

In this scenario, the number of nodes is vary in range of: 50, 60, 70, 80, 90,100 by keeping maximum speed 5 m/s, pause time 5 sec and number of connections 10. Results are taken with different scenario files having same parameters.

Test 1: Varying number of nodes

i) Average Consumed Energy (J)

The graph shown in the diagram shows the main differences between the typical scenario, the WSN attack and the proposed scheme. With the use of the proposed framework, energy consumption has been reduced.

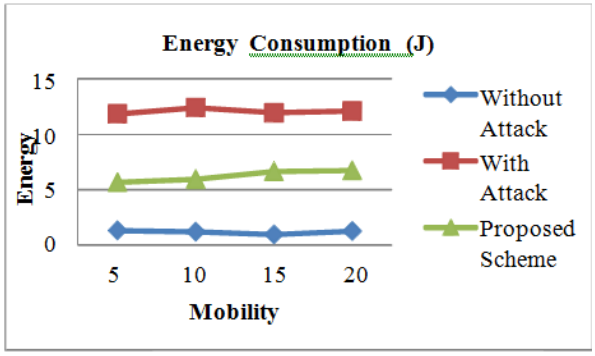

Fig. 3. Energy Consumption vs. Number of Nodes

ii) Packet Delivery Ratio (PDR) (%)

The graph in the figure shows that, in the AODV and before the attack, the PDR is proportional to the number of nodes. But the value of the PDR decreases with the presence of attacks of the ideal scenario. With the proposed work structure, the RDP has increased compared to the assault scenario.

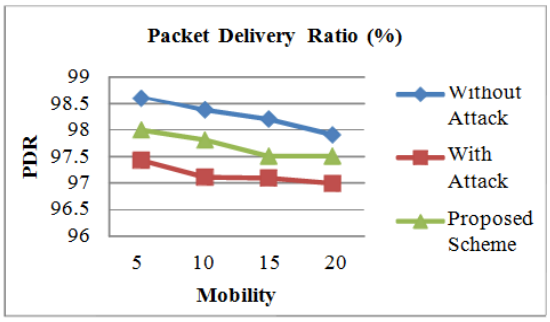

Fig. 4. PDR vs. Number of Nodes

iii) Routing Overhead

The graph shown in the figure concludes that the overhead routing to AODV is lower than the WSN attack. The value increases as the number of nodes increases. The routing time increases with the proposed scheme, which can be considered as a limitation of this work.

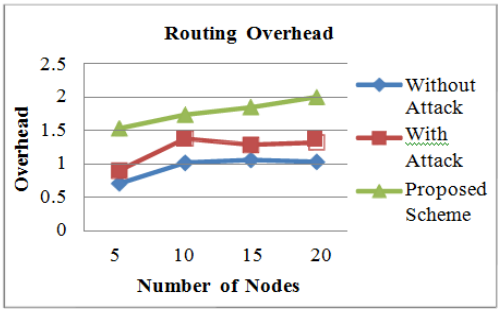

Fig. 5. Routing Overhead vs. Number of Nodes

Test 2: Varying the mobility

In this scenario, varying the value of mobility in range of: 5, 10, 15, 20 by keeping the number of nodes constant as 50, pause time 5 sec, and number of connections 5.

i) Average Consumed Energy (J)

The graph below shows the radical change between the normal scenario and the attack scenario, as well as the proposed method improvements. Inside the presence of the WSN attack force is proportional to its mobility.

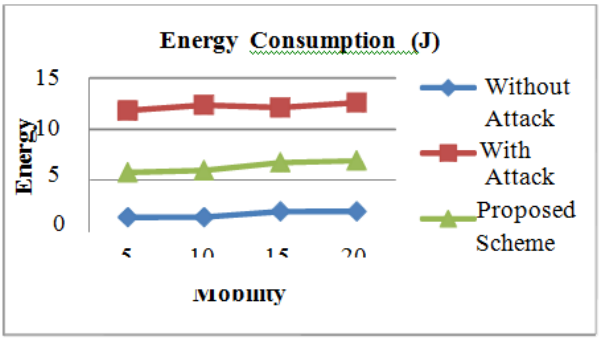

Fig. 6. Energy Consumption vs. Mobility

ii) Packet Delivery Ratio (PDR) (%)

The graph shown in the figure shows that in AODV and before the attack, the RDP is proportional to mobility. But the value of the PDR decreases with the presence of attacks of the ideal scenario.

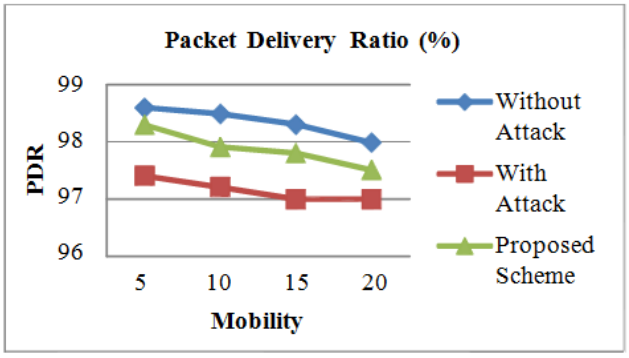

Fig. 7. PDR vs. Mobility

iii) Normalized Routing Overhead

The graph shown in the figure concludes that in the OVC and before the attack, the routing of overhead is proportional to the mobility. It was also concluded that the proposed framework has the highest overhead costs.

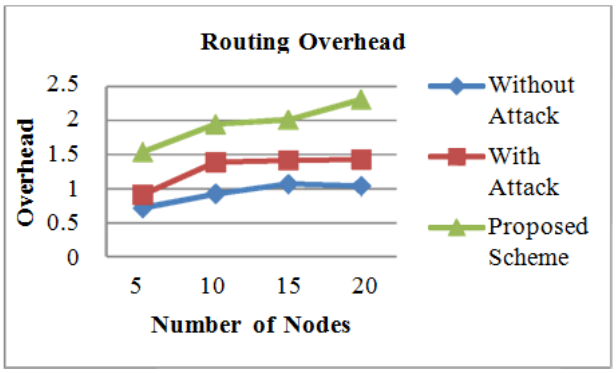

Fig. 8. Routing Overhead vs. Mobility

VI. CONCLUSION

This paper discusses energy-consuming attacks and their effects on wireless sensor networks. In WSN, it is important to focus on energy issues because if the network is protected from further attack, the power or network network is weaker. WSN attacks are attacks that use the battery life and energy of a network node. This attack classification is based on the routing protocol used in the network. The WSN attack is not protocol specific, so it is impossible to predict its presence on the network.

Simulate ideal scenarios and scenarios with WSN the attack was carried out. And we have also implemented this proposal framework that combines MST and RC5. Graphical analysis such as PDR, Overhead routing and Energy consumption compared to some nodes mobility. From the foregoing, the work is done and done extensively Bibliographic Survey We have come to the conclusion that by using a minimum spanning tree, it may be able to limit the damage done to this type of attack and we could also protect against other attacks by encrypting via RC5. We do not offer a satisfactory solution to the WSN attack, but we suggest some information about possible damage caused by encryption techniques and shorter energy-based routes. But this method affects the routing system time. As a result, alternative solutions to these attacks are left for future work that may limit the value of the routing overhead. The elimination of defects and defects for topological discoveries can also be improved in the future.

REFERENCES

1. Potdar, Vidyasagar, Atif Sharif, and Elizabeth Chang. "Wireless sensor networks: A survey." Advanced Information Networking and Applications Workshops, 2009. WAINA'09. International Conference on. IEEE, 2009.
2. Pandey, Abhishek, and R. C. Tripathi. "A survey on wireless sensor networks security." International Journal of Computer Applications 3.2 (2010): 43-49.
3. Padmavathi, Dr G., and Mrs Shanmugapriya. "A survey of attacks, security mechanisms and challenges in wireless sensor networks." arXiv preprint arXiv:0909.0576 (2009).
4. Ishmanov, Farruh, Aamir Saeed Malik, and Sung Won Kim. "Energy consumption balancing (ECB) issues and mechanisms in wireless sensor networks (WSNs): a comprehensive overview." European Transactions on Telecommunications 22.4 (2011): 151-167.
5. Abirami, R., and G. Premalatha. "Depletion of WSN attacks in medium access control level using interior gateway routing protocol." Information Communication and Embedded Systems (ICICES), 2014 International Conference on. IEEE, 2014.
6. Mariyappan, E., and C. Balakrishnan. "Power draining prevention in Ad-Hoc Sensor networks using sensor network encryption protocol." Information Communication and Embedded Systems (ICICES), 2014 International Conference on. IEEE, 2014.
7. Deshmukh, Lina R., and A. D. Potgantwar. "Ensuring an early recognition and avoidance of the WSN attacks in WSN using routing loops." Advance Computing Conference (IACC), 2015 IEEE International. IEEE, 2015.
8. V. Arulkumar. "An Intelligent Technique for Uniquely Recognising Face and Finger Image Using Learning Vector Quantisation (LVQ)-based Template Key Generation." International Journal of Biomedical Engineering and Technology 26, no. 3/4 (February 2, 2018): 237-49. doi:10.1504/IJBET.2018.089951.
9. Reddy, K. Shyam Sundar, and GS Prasada Reddy. "Securing Data Packets from WSN Attacks in Wireless Ad-hoc Sensor Network."
10. Anand, Jose, and K. Sivachanda. "WSN Attack Detection in Wireless Sensor Network." International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3 (2014).
11. Patel, Manish M., and Akshai Aggarwal. "Security attacks in wireless sensor networks: A survey." Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on. IEEE, 2013.
12. Rivest, Ronald L. "The RC5 encryption algorithm." Fast Software Encryption. Springer Berlin Heidelberg, 1994.
13. Gawali, Dhanashri H., and Vijay M. Wadhai. "Rc5 algorithm: potential cipher solution for security in wireless body sensor networks (WBSN)." International Journal Of Advanced Smart Sensor Network Systems, AIRCC 2.3 (2012): 1-7.
14. Sasi, Swapna B., et al. "A general comparison of symmetric and asymmetric cryptosystems for WSNs and an overview of location based encryption technique for improving security." IOSR Journal of Engineering 4.3 (2014): 1.
15. Mitali, Vijay Kumar, and Arvind Sharma. "A survey on various cryptography techniques." International Journal of Emerging Trends and Technology in Computer Science 3.4 (2014): 6.
16. V Arulkumar, Charlyn Puspha Latha, Daniel Jr Dasig, "Concept of Implementing Big Data In Smart City: Applications, Services, Data Security In Accordance With Internet of Things and AI" International Journal of Recent Technology and Engineering 8, no. 3 (September 2019): 237-49.
17. Ganesan, Prasanth, et al. "Analyzing and modeling encryption overhead for sensor network nodes." Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications. ACM, 2003.
18. Mittal, Trisha, and Bijendra Kumar. "NONACK in wireless ad hoc network."Computational Intelligence on Power, Energy and Controls with their impact on Humanity (CIPECH), 2014 Innovative Applications of. IEEE, 2014.

19. Ganesan, Prasanth, et al. "Analyzing and modeling encryption overhead for sensor network nodes." Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications. ACM, 2003.
20. Poonkodi R, Geetharani M, Gunasekaran R," Automatic Lobar Segmentation Algorithm for Pulmonary Lobes from Chest Ct Scans Based On Fissures and Blood Vessels" International Journal of Innovative Research in Computer and Communication Engineering, 2320-9798, April 2015.

AUTHORS PROFILE

R.Poonkodi, she currently working as Assistant Professor, Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore and Perusing PhD degree in Information and Communication Engineering in Anna University Chennai. She was born in Tiruppur, Tamilnadu, India, in 1985. She received the B.Tech degree in Information Technology from Maharaja Engineering College, Avinashi, India, in 2006, and the M.E degrees in Computer Science and Engineering from Sasurie College Of Engineering, Erode, India, in 2013, respectively. Her research interest includes wireless sensor network, Cloud Technology. She has published many research papers in National/International Conferences and Journals. She has attended several seminars and workshops in the past 5 years.

Dr. N. SaravanaSelvam, Professor, Department of ECE, PSR Engineering College, Sevalpatti, Sivakasi. He has obtained his Ph.D. in Computer Science and Engineering from Anna University, Chennai in the year 2013. He has obtained both of his Post Graduate degree, M.E. (Computer Science and Engineering) and Graduate degree B.E., (Electronics and Communication Engineering) from Madurai Kamaraj University (Tamilnadu, India). During his twenty years of teaching profession, he shouldered a member of teaching, administrative and societal based assignments. He is a Life Member of ISTE, IAEng and IACSIT. Currently, he is specializing in the area of Network Engineering, Data Mining and IoT. He has published more than 30 papers in international journals.