


# Security in Wireless Sensor Networks: Issues and Challenges

**A.P. Thangamuthu**

*Assistant Professor of Computer Technology*

*Sri Krishna Adithya College of Arts & Science, Coimbatore, Tamil Nadu, India*

 <https://orcid.org/0000-0001-5804-2682>

## OPEN ACCESS

Manuscript ID:

ASH-2021-08043671

Volume: 8

Issue: 4

Month: April

Year: 2021

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Received: 20.01.2021

Accepted: 04.03.2021

Published: 01.04.2021

Citation:

Thangamuthu, AP.  
"Security in Wireless  
Sensor Networks: Issues  
and Challenges." *Shanlax  
International Journal  
of Arts, Science and  
Humanities*, vol. 8, no. 4,  
2021, pp. 120-128.

DOI:

<https://doi.org/10.34293/sijash.v8i4.3671>



This work is licensed  
under a Creative Commons  
Attribution-ShareAlike 4.0  
International License

## Abstract

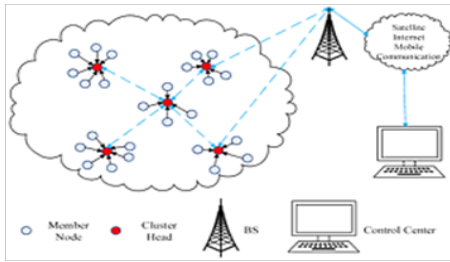
*Wireless sensor networks (WSNs) have made it easier for people to live in various fields: medical engineering, agriculture. With computing power and wireless networking, sensing technology makes it lucrative for its potential abundance of use. Since the many uses of such systems have been used, lightweight, inexpensive, disposable and self-contained computers, known as sensor nodes or "motes," are created. WSNs are commonly used in applications for monitoring, tracking and control. These include centralized management, system heterogeneity, protocol routing, the versatility of node, the privacy of information and restricted computing capacity. WSN covers a wide geographical area; routing protocols, scalability and security should therefore be addressed. In the traditional networking technique, there are major benefits due to the low cost and cooperative design of wireless networks (WNS). The networks with wireless sensors have more advantages over wired networks. Although wireless networks have various advantages, they are vulnerable to security problems. Due to the broader application, safety has become an important issue for wireless sensor networks.*

**Keywords:** Sensor, Communication, Application, Device, Information, Protocol, Security, Wired, Wireless

## Introduction

Wireless Sensor Networks (WSNs) can be described as self-configured and infrastructure-free wireless networks for monitoring physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or contaminants, temperature, pressure, humidity, soil composition, vehicular motion, noise, lighting conditions, the existence or absence of certain types of artifacts or substances, etc. Usually, a wireless sensor network consists of hundreds of thousands of sensor nodes. The sensor nodes will communicate with each other using radio signals. The wireless sensor node is fitted with sensing and computing facilities, radio transceivers and control components.

Traditionally, sensors are connected to the environment and their readings are transmitted to a wired base station (BS). In recent years, a new vision of sensor nodes has arisen as autonomous systems with advanced sensing, processing and communication capabilities. The attachment of the antenna for transmitting signals and the transmitter allows wireless contact of the sensors. Sensors often have a fast processor and a small memory for encoding and decoding signals. Recent developments in electronics and wireless network technology have provided us access to a new age in which wireless sensor networks created by interconnected lightweight, intelligent sensing devices give us the ability to build smart environments.



**Figure 1: Wireless Sensor Networks**

The primary purpose of sensor networks is to provide:

- Timely reliable reports on the condition of the plant so that the plant can function with optimum productivity.
- Data for scientists as part of a dynamic experiment.
- Data for the checking and inspection of components before they are placed into service

Wireless Sensor Networks (WSNs) are characterized as a wide number of low-cost, low-record, self-organizing, unattended, low-processing, and distributed embedded small sensor nodes; they communicate via a channel (air) to capture, process and report data from the surrounding interest.

### Why used Wireless Networks?

Wireless networks offer following six advantages when compared to traditional wired networks:

**Increased Mobility:** Wireless networks allow smartphone customers to view the information in real-time so that they can travel across the company's room without being removed from the web. This increases company-wide collaboration and competitiveness that is not feasible for conventional networks.

**Installation Speed and Simplicity:** Installing a wireless network infrastructure eliminates the number of cables that are difficult to put up and can pose a safety danger should workers fly. It can also be built efficiently and reliably relative to a conventional network.

**Wider Reach of the Network:** The wireless network will be expanded to areas within the enterprise that not open to wires or cables.

**More Flexibility:** If your network improves in the future, you can quickly upgrade your wireless network to suit new configurations.

**Reduced Cost of Ownership over Time:** Wireless networking can result in a marginally higher initial investment, but average costs are smaller. It can also have a longer lifecycle than a conventional network.

**Increased Scalability:** Wireless networks may be designed uniquely to suit the needs of particular applications. They can be adjusted and scaled quickly depending on the organization's needs.

### Types of Network

#### Wired Networks

“Wired” implies any physical medium composed of wires. There may be copper wire, twisted pair, or fiber optic cables. The wired network is used to transport various types of electrical signals from one end to the other. Often, in a wired network, one internet connection is made using a T1 line, a cable modem, or some other means. This communication is shared between different devices using a wired network concept.

LAN (Local Area Network): this network consists of Ethernet cards stored on PCs or laptops. These cards are linked via Ethernet cables. The data is streaming between these cards. A limited number of desktop or notebook computers are attached to a small wired network router. Different switches and routers are used to expand network coverage with more networks.



**Figure 2: Wired Network**

#### Wireless Networks

“Wireless” is the term used to mean electromagnetic waves (i.e., EM waves) or infrared waves. Both wireless systems are fitted with an antenna or sensors. Typical wireless products include smartphones, wireless sensors, remote TVs, satellite dish receivers, notebooks with WLAN cards, etc.

The wireless network does not use cables for data or voice communication; it uses radio frequency waves as indicated above. Other examples include fiber optic networking and ADSL broadband, etc.

### Examples of Wireless Network

1. Cellular outdoor technology such as GSM, CDMA, WiMAX, LTE, Satellite, etc.
2. Wireless indoor technology such as wireless LAN (or WiFi), Bluetooth, IrDA, Zigbee, Zwave, etc.



Figure 3: Wireless Network

### Wireless Sensor Networks

The Wireless Sensor Network (WSN) is a wireless network infrastructure that is implemented in many wireless sensors in an ad hoc fashion that is used to track device, physical or environmental conditions. Sensor nodes are used in WSN with an on-board processor that controls and tracks the environment in a specific region. They are linked to the Base Station, which serves as a processing unit in the WSN system. The base station in the WSN system is connected to exchange data over the Internet.

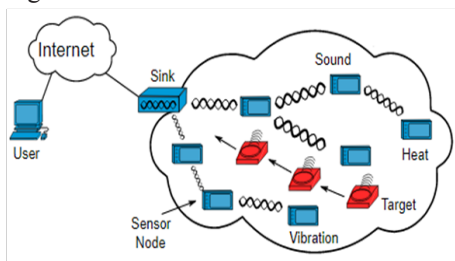


Figure 4: Wireless Sensor Network

### WSN Architecture

The most popular WSN architecture is the OSI architecture model. The WSN architecture consists of five layers and three layers. Mostly in sensor n/w, we need five layers, i.e., application, transport, n/w, data link and physical layer. The three cross-planes are control management, agility management and

mission management. These layers of the WSN are used to do the n/w and allow the sensors to work together to improve the overall performance of the network.

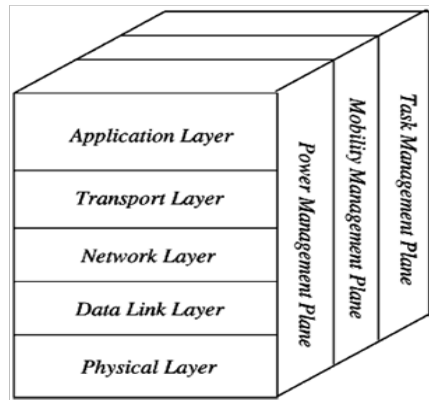


Figure 5: Wireless Sensor Network Architecture

### Application Layer

The application layer is responsible for traffic control and provides tools for a wide variety of applications that translate data in a simple way to locate positive details. Sensor networks have been set up in various applications in diverse areas, such as agriculture, military, environmental, medical, etc.

### Transport Layer

The role of the transport layer is to ensure the prevention and stability of congestion where a lot of protocols designed to provide this function are either realistic on the upstream side. These methods use various procedures for the identification of losses and recovery of losses. The transport layer is required when a system is designed to access other networks.

Providing stable loss recovery is more energy consuming and is one of the key reasons why TCP is not suited to WSN. In general, the layers of transport can be divided into a packet-based, event-driven. There are some common transport layer protocols, namely STCP (Sensor Transmission Control Protocol), PORT (Price-Oriented Reliable Transport Protocol) and PSFQ (pump slow fetch quick).

### Network Layer

The key function of the network layer is routing, it has several application-based tasks, but really, the

main tasks are power conservation, partial memory, buffers, and sensors that do not have a common ID and need to be self-organized.

The basic principle of the routing protocol is to describe a stable lane and redundant lanes on a persuaded scale called a metric, which differs from protocol to protocol. There are many existing protocols for this network layer, which can be divided into; flat routing and hierarchical routing or can be separated into time-driven, query-driven and event-driven.

### Data Link Layer

The data link layer is responsible for multiplexing data frame recognition, data streams, MAC, & error management, confirming the efficiency of point to point(s) to point.

### Physical Layer

The physical layer includes the edge for the transfer of a stream of bits above the physical medium. This layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation & data encryption. Wireless network sensor with low cost, power usage, density, range of contact to boost battery life.

### Applications of WSN

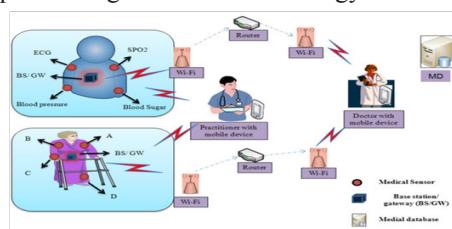
Wireless sensor networks may consist of various types of sensors, such as low sampling rate, seismic, magnetic, thermal, optical, infrared, radar and acoustic, which are cleverly designed to track a wide range of environmental circumstances. Sensor nodes are used for continuous sensing, event ID, event monitoring & local actuator control. Uses of wireless sensor network include primarily fitness, military, environmental, home & other commercial fields.

- Military Applications
- Environmental Applications
- Home Applications
- Commercial Applications
- Area monitoring
- Environmental/Earth sensings
- Air pollution monitoring
- Forest fire detection
- Landslide detection
- Water quality monitoring

**Education** - Many colleges and elementary schools consider valuable reasons to add wireless LANs, mainly to provide their students with mobile network apps. Schools have started to take advantage of the presence of wireless LAN connectivity as a strategic advantage. These schools target a rising number of students with laptops and aspirations for access to the Internet and school services from everywhere on campus, such as labs, libraries, quads and dormitories. Students can conveniently update e-mail, surf the internet, access advanced school apps, check scores, and view transcripts. As a result, students are making greater use of their time.

**Inventory Control** - Many industries benefit from using wireless LANs to handle their production processes. It decreases the running expenses. Since the communications between the production equipment and the main control systems are digital, the organization can reconfigure the assembly process from anywhere at any moment, saving time and resources. Using a wireless LAN, an organization can monitor and upgrade inventory in real-time, allowing productivity and accuracy to improve significantly. In the retail world, as soon as a clerk orders or shops a product, a wireless monitoring solution will change the inventory. In the production environment, the organization should keep raw materials and finished product data up to date. Employees fitted with wireless barcode scanners can verify or adjust merchandise prices or check the number in stock.

**Health care monitoring** - Health care sensors now play a vital role in hospitals. The patient tracking system is one of the big advances due to its innovative technologies. The automated wireless health tracking device is used to track the patient's body temperature and pulse using embedded technology.



**Figure 6: Health Care Monitoring System**

**Industrial monitoring** - Industrial automation systems have been common in many industries and

play a key role in managing various process-related operations. As a result of introducing a wide range of industrial networks with their regional delivery through the plant or market, transmission and control capacity of floor data has become more complex and simple, varying from low-level to high-level control.



**Figure 7: Industrial Monitoring System**

**Public Networks** - Due to the significant distribution of tablets, PDAs and cell phones, there is a growing need for mobile Internet and corporate interfaces. Users want and anticipate smooth, continuous mobile access to all information sources with high efficiency and availability. Wireless networks provide resources to meet these demands in public places away from home or workplace.

A public wireless network provides a way for people on the move to connect to the Internet. In general, areas with large numbers of people who need or want network connectivity provide wireless LAN access. Wireless MANs and WANs, on the other hand, have coverage over wider territories of sparsely scattered populations. Public wireless LANs are popular sites, such as hotels and bars, but all areas have wireless LANs for public access.

### Challenges of WSN

WSNs are subject to many constraints, such as limited processing capacity, limited memory, fewer energy resources, susceptibility to physical capture and lack of infrastructure, which make them vulnerable to many security threats or problems and make security tactics unavoidable and attractive for certain security solutions. The wireless sensor network is a specific network with certain drawbacks relative to the conventional computing network.

**Wireless Medium:** The wireless media is less safe because its nature of broadcasting makes eavesdropping easy.

**Ad-Hoc Deployment:** The ad-hoc design of the sensor networks ensures that no configuration can be statically described. Network topology is often subject to change due to malfunction, extension, or mobility of the node. Nodes can be deployed by airdrop, but little is understood about the topology before deployment. Since nodes can malfunction or be replaced, the network must allow self-configuration.

**Hostile Environment:** The next challenge is the hostile world in which the sensor nodes run. Since nodes can be in a hostile environment, attackers can quickly obtain physical access to the computers.

**Resource Scarcity:** The intense resource constraints of sensor systems pose major challenges to resource-hungry protection mechanisms.

**Immense Scale:** Simply networking tens to hundreds or thousands of nodes has proved to be a huge challenge. Protection mechanisms must apply to very large networks while retaining high computational and communication efficiency.

**Unreliable Communication:** Certainly, unreliable contact is another threat to the protection of the sensor. Network security relies heavily on a given protocol, which in turn depends on communication.

**Unreliable Transfer:** Normally, the packet-based routing of the sensor network is unconnected and thus potentially inefficient.

**Conflicts:** Even if the medium is secure, communication will also be inconsistent. This is due to the existence of the wireless sensor network.

**Latency:** Multi-hop routing, network congestion and node processing may contribute to greater network latency, rendering it difficult to achieve synchronization across sensor nodes.

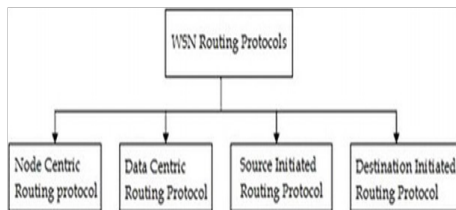
**Unattended:** Operation Depending on the role of the individual sensor network, the sensor nodes can be left unattended for a long period. There are three key warnings to unattended sensor nodes

**Managed Remotely:** The remote control of the sensor network makes it nearly difficult to detect physical tampering and physical repair problems.

**No Central Management Point:** A sensor network should be a distributed network without a central control point. This would increase the vitality of the network of sensors. However, if poorly built, the organization of the network would be complicated, inefficient and delicate.

**Routing Protocols**

Routing protocols are used for the dissemination of routing information between routing devices. This information can shift overtime on the basis of network conditions; thus, this information is crucial to ensuring that packets reach their destinations. Of necessity, attackers may use routing protocols for attacks as well. For, eg, it could be called a Denial-of-Service (DoS) attack to maliciously set routes so that a certain network cannot be accessed.



**Sensor protocols for information via negotiation (SPIN)**

- This protocol is specified to be used to eliminate a deficiency such as flooding and gossip that exists in other protocols. The key point is that the exchange of data, which is sensed by the node, would require more resources than the meta-data, which is just a descriptor of the node’s data.

**Data-centric** - In most wireless sensor networks, sensed data or information is much more important than the real node itself. Therefore, data-centric routing strategies are the primary objective of transferring information identified by certain attributes rather than the collection of data from certain nodes.

**Directed diffusion (DD)** - Directed diffusion is a data-based routing strategy. This data-centric methodology is used to collect and circulate information. This routing protocol is also an energy-efficient and energy-saving protocol, so the life of the network is improved.

**Security Schemes in Wireless Sensor Networks**

**Cryptography:** The basic security mechanism for wireless sensor networks is cryptography, which directly protects data. In short, cryptography is a series of techniques for translating the original information into a set of unreadable data, allowing it to be interpreted only by the right receiver. Due to all constraints inherent to wireless sensor networks, particularly when processing and distributing multimedia data, conventional cryptography with high computation and overhead communication might not be feasible for WSN.

**Steganography:** Network steganography is a covert networking tactic that uses legal traffic as a vehicle to secretly transfer classified information over an untrusted network. Bit Torrent (BT) is one of the most common P2P services for sharing video files over wireless networks.

**Data Availability:** Data availability is a term used by some computer storage manufacturers and storage service providers (SSPs) to describe products and services that ensure that data continues to be available at the required level of performance in situations ranging from normal to “disastrous.” In general, data availability is achieved through redundancy involving where the data is stored and how it can be accessible.

**Data Confidentiality:** Data security concerns data security against accidental, improper, or unwanted entry, leak, or robbery. Confidentiality has to do with the protection of records and the freedom to access, exchange and use them.

**Data Integrity:** It refers to the precision and continuity (validity) of the data over its lifetime. After all, the stolen record was of no benefit to businesses, not to mention the threats faced by the destruction of confidential data. For this cause, preserving data privacy is a primary priority of many corporate protection strategies.

**Attacks in Wireless Sensor Networks**

**Denial of Service:** It is an intrusion designed to shut down a computer or network, making it unavailable to its intended users. DoS attacks do this by overwhelming the target with traffic or by giving it information that causes a crash. DoS is a security

threat when an intruder blocks acceptable users from accessing certain computers, operating networks, or other cloud-based IT services. DoS attacks are quick but effective and can inflict extreme harm to cloud infrastructure and facilities, often attacking the bandwidth or connectivity of computer networks. With one attack, the cloud protection of an enterprise may be compromised for days or even weeks, and servers may become inaccessible to all computers and users around the network.

**Attacks on Information in Transit:** Cyber assault is some sort of malicious activity aimed at electronic information systems, infrastructures, computer networks, or personal computer equipment, using a range of tactics to steal, modify or destroy data or information systems.

**Sybil Attack:** The assault starts with the development of a vast number of identities. The quicker it is to create them, the simpler it is to create bigger numbers, weakening the peer-to-peer network credibility mechanism. The crucial part is the degree to which the credibility mechanism accepts inputs from nodes that do not have a chain of confidence connecting them to known, trustworthy nodes.

**Blackhole Attack:** It happens when an intermediary collects and re-programs a series of nodes in the network to block/drop packets and produces false signals instead of transmitting correct/true information to the base station in the wireless sensor network.

**Hello Flood Attack:** Hello flood attack is an attack on the network layer. An adversary node broadcasts high transmission capacity packets such that most of the nodes on the network pick it as a cluster header.

**Wormhole Attack:** In a wormhole attack, an attacker records packets (or bits) at one location on the network, tunnels them (possibly selectively) to another location transmits them back to the network.

### Research Progress of Wireless Sensor Networks Security

**Authentication:** The introduction of authentication helps you to encrypt a network such that only users with the correct certificate can access network services. Provides authentication by user name and

password and helps you to set the user's privileges on the network. It's not an all-or-nothing issue, of course; you can use authentication to limit or allow what a single user can do while within the network.

**Key Management:** Key control is one of the most critical tasks of the wireless mesh network. This service is responsible for the generation, delivery, and sharing of keys in a cryptographic scheme.

**Intrusion Detection:** The Intrusion Detection System (IDS) is a software or hardware mechanism used to detect unwanted access to a computer system or network. A wireless IDS performs this role solely on a wireless network. These devices track traffic on the network watching for and recording risks and alerting workers to respond.

**Privacy Protection:** Wireless protection is the avoidance of unauthorized access to devices over wireless networks. Wired Alternative Privacy (WEP) and Wi-Fi Safe Connectivity are the most common forms of wireless protection (WPA). WEP is a notoriously poor safety norm.

**Security Management:** Network protection is the practice of using physical and software security solutions to defend the underlying network infrastructure from unwanted access, abuse, failure, alteration, disruption, or inappropriate disclosure, & to establish a protected forum for machines, users, & programs to execute their tasks in a secure setting.

### Conclusions

Wireless sensor networks are increasingly used in military, environmental, health, and industrial applications. Sensor networks are fundamentally distinct from conventional wired networks as well as ad-hoc wireless networks. Protection is an essential aspect of the implementation of wireless sensor networks. Many vulnerability breaches in wireless sensor networks are triggered by introducing false information by infected nodes within the network. To protect the inclusion of false reports by compromised nodes, a means of detecting false reports is necessary. Protection in the Wireless Sensor Network is important for the adoption and utilization of sensor networks. Specifically, the Wireless Sensor Network product in the market will not be approved until there is complete evidence of protection on the network.

## References

- Akyildiz, I.F., et al. "A Survey on Sensor Networks." *IEEE Communications Magazine*, vol. 40, no. 8, 2002, pp. 102-114.
- Akyildiz, I.F., et al. "Wireless Sensor Networks: A Survey." *Computer Networks*, vol. 38, no. 4, 2002, pp. 393-422.
- Alam, Sahabul, and Debashis De. "Analysis of Security Threats in Wireless Sensor Network." *International Journal of Wireless & Mobile Networks*, vol. 6, no. 2, 2014, pp. 35-46.
- Anwar, Raja Waseem, et al. "Security Issues and Attacks in Wireless Sensor Network." *World Applied Sciences Journal*, vol. 30, no. 10, 2014, pp. 1224-1227.
- Chelli, Kahina. "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures." *Proceedings of the World Congress on Engineering*, 2015.
- Chowdhury, Mahfuzulhoq, et al. "Security Issues in Wireless Sensor Networks: A Survey." *International Journal of Future Generation Communication and Networking*, vol. 6, no. 5, 2013, pp. 97-116.
- Dai, Shijin, et al. "Research and Analysis on Routing Protocols for Wireless Sensor Networks." *International Conference on Communications, Circuits and Systems*, 2005.
- Dirk, Westhoff, et al. *Security Solutions for Wireless Sensor Networks*.
- Franklin, Matthew, et al. "Eavesdropping Games: A Graph-theoretic Approach to Privacy in Distributed Systems." *Journal of the ACM*, vol. 47, no. 2, 2000.
- Heinzelman, W.R., et al. "Energy-efficient Communication Protocol for Wireless Microsensor Networks." *Proceedings of the 33rd Hawaii International Conference on System Sciences*, 2000.
- Hiremani, Vani, and Monali Madne. "Security Mechanism for Wireless Sensor Networks - A Review." *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 1, 2013, pp. 915-918.
- Kaplantzis, Sophia. *Security Models for Wireless Sensor Networks*. 2006.
- Karlof, Chris, and David Wagner. "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures." *Ad Hoc Networks*, vol. 1, no. 2-3, 2003, pp. 293-315.
- Khare, Poonam, and Sara Ali. "Survey of Wireless Sensor Network Vulnerabilities and its Solution." *International Journal of Recent Development in Engineering and Technology*, vol. 2, no. 6, 2014, pp. 84-88.
- Kumar, Vikash, et al. "Wireless Sensor Networks: Security Issues, Challenges and Solutions." *International Journal of Information & Computation Technology*, vol. 4, no. 8, 2014, pp. 859-868.
- Liu, Donggang and Peng Ning. "Multi-level  $\mu$ TESLA: Broadcast Authentication System for Distributed Sensor Networks." *ACM Transactions on Embedded Computing Systems*, 2004, vol. 3, no. 4, 2004.
- Lupu, Teodor-Grigore. *Main Types of Attacks in Wireless Sensor Networks*.
- Manjeshwar, A., and D.P. Agrawal. "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks." *Proceedings of 15th International Parallel and Distributed Processing Symposium*, 2001.
- Modares, Hero, et al. "Overview of Security Issues in Wireless Sensor Networks." *Third International Conference on Computational Intelligence, Modelling & Simulation*, 2011.
- Naeem, Tahir, and Kok-Keong Loo. "Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks." *International Journal of Digital Content Technology and its Applications*, vol. 3, no. 1, 2009, pp. 88-93.
- Pathan, A.S.K., et al. "Security in Wireless Sensor Networks: Issues and Challenges." *International Conference Advanced Communication Technology*, 2006.
- Pathan, Al-Sakib Khan, et al. "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks." *IEEE ICNEWS*, 2006, pp. 282-286.
- Pathan, Al-Sakib Khan, et al. "Security in Wireless Sensor Networks: Issues and Challenges." *ICACT2006*, 2006, pp. 1043-1048.



- Pathan, Al-Sakib Khan, et al. "Security in Wireless Sensor Networks: Issues and Challenges." *International conference Advanced Communication Technology*, 2006.
- Perrig, Adrian, et al. "Security in Wireless Sensor Networks." *Communications of the ACM*, vol. 47, no. 6, 2004, pp. 53-57.
- Perrig, Adrian, et al. "SPINS: Security Protocols for Sensor Networks." *Wireless Networks*, vol. 8, 2002, pp. 521-534.
- Rajasegarar, Sutharshan, et al. "Anomaly Detection in Wireless Sensor Networks." *IEEE Wireless Communications*, vol. 15, 2008, pp. 34-40.
- Ramen, Rodrigo, et al. "Situation Awareness Mechanisms for Wireless Sensor Networks." *IEEE Communications Magazine*, vol. 46, no. 4, 2008, pp. 102-107.
- Reddy, Alla Chandra Sekhar, and Riaz Shaik. "Effective Detection of Denial of Service (Dos) Attacks by Using Snort Rules Architecture." *International Journal of Applied Engineering Research*, vol. 9, no. 19, 2014, pp. 1635-1646.
- Saleh, Mohammad, and Iyad Al Khatib. "Throughput Analysis of WEP Security in Ad Hoc Sensor Networks." *The Second International Conference on Innovations in Information Technology (IIT'05)*, 2005.
- Santhi, G., and R. Sowmiya. "A Survey on Various Attacks and Countermeasures in Wireless Sensor Networks." *International Journal of Computer Applications*, vol. 159, no. 7, 2017, pp. 7-11.
- Sarma, Hiren Kumar Deva, and Avijit Kar. "Security Threats in Wireless Sensor Networks." *IEEE Aerospace and Electronic Systems Magazine*, vol. 23, no. 6, 2008, pp. 39-45.
- Shaik, Riaz, et al. "Sufficient Authentication for Energy Consumption in Wireless Sensor Networks." *International Journal of Electrical and Computer Engineering*, vol. 6, no. 2, 2016, pp. 735-742.
- Sharma, Kalpana, and M K Ghose. "Wireless Sensor Networks: An Overview on its Security Threats." *IJCA Special Issue on Mobile Ad-hoc Networks*, 2010, pp. 42-45.
- Shi, E., and A. Perrig. "Designing Secure Sensor Networks." *IEEE Wireless Communications*, vol. 11, no. 6, 2004, pp. 38-43.
- Undercoffer, Jeffery, et al. "Security for Sensor Networks." *CADIP Research Symposium*, 2002.
- Venkataraman, K., et al. "Various Attacks in Wireless Sensor Network: Survey." *International Journal of Soft Computing and Engineering*, vol. 3, no. 1, 2013, pp. 208-211.
- Walters, John Paul, et al. "Wireless Sensor Network Security: A Survey." *Security in Distributed, Grid, and Pervasive Computing*, Auerbach Publications, 2006.
- Wang, Yong, et al. "A Survey of Security Issues in Wireless Sensor Networks." *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, 2006, pp. 2-23.
- Xu, Wenyuan, et al. "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks." *Mobile Ad Hoc Networking and Computing*, 2005, pp. 46-57.
- Yu-Long, Shen, et al. "MM $\mu$ TESLA: Broadcast Authentication Protocol for Multiple-Base-Station Sensor Networks." *Chinese Journal of Computers*, 2007, pp. 539-546.
- Zhang, Yan, and Paris Kitsos. *Security in RFID and Sensor Networks*. Routledge, 2009.
- Zhou, Yun, et al. "Securing Wireless Sensor Networks: A Survey." *IEEE Communications Surveys & Tutorials*, vol. 10, 2008, pp. 6-28.

### Author Details

**A.P. Thangamuthu**, Assistant Professor of Computer Technology, Sri Krishna Adithya College of Arts & Science, Coimbatore, Tamil Nadu, India, **Email ID:** a.p.thangamuthu@gmail.com