OPEN ACCESS

Manuscript ID:
ASH-2021-09024159

Volume: 9

Issue: 2

Month: October

Year: 2021

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Received: 07.07.2021

Accepted: 05.09.2021

Published: 01.10.2021

Citation:
Thangamuthu, AP. "A Survey on Various Attacks and Countermeasures in Wireless Sensor Networks." *Shanlax International Journal of Arts, Science and Humanities*, vol. 9, no. 2, 2021, pp. 26–34.

DOI:
https://doi.org/10.34293/sijash.v9i2.4159

A Survey on Various Attacks and Countermeasures in Wireless Sensor Networks

A. P. Thangamuthu
Assistant Professor of Information Technology
Sri Krishna Adithya College of Arts & Science, Coimbatore, Tamil Nadu, India
https://orcid.org/0000-0001-5804-2682

Abstract

The Wireless Sensor Network (WSN) is an evolving technological base comprising spatially dispersed, autonomous tiny sensing devices called nodes. Today, wireless sensor networks are not exclusively limited to military uses such as frontline surveillance. However, they are still used in various industrial and civilian applications, including industrial process tracking and operation, robotic health monitoring, vibration and flame monitoring, healthcare systems, home automation, and traffic management. Nodes, such as temperature, hermetic, vibration, pressure, leisure seizure, or pollutant parameters, are deployed independently to cooperatively control mammal or environmental conditions. The compulsion of security issues occurs in the Wireless Sensor Network to be accepted with complete zip honesty, confidentiality, authentication during contact. In this paper, we analyze the security criteria, internal and external security threats and attacks that can be done, and the mechanism used in the Wireless Sensor Network to address such security issues.

Keywords: Wireless Sensor Network, Security, GKM, Application, Communication

Introduction

Since they are theoretically low-cost alternatives to several real-world problems, wireless sensor networks are quickly gaining prominence. Advances in wireless networking and the implementation of electronic technology have made the production of low-cost, low-power, multi-functional sensor nodes feasible. These nodes are limited in size and interact over short distances. These small sensor nodes, consisting of sensing, data collection, and communication components, make use of the concept of sensor networks.

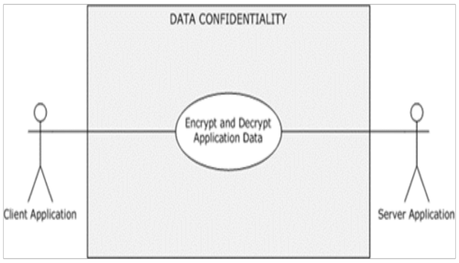
Sensor networks are an essential factor in supporting more than defined sensors. A sensor network consists of many tiny nodes of the sensor that are either densely deployed inside the phenomenon or totally stuffy to each other Data and partly analyzed. This facilitates the use of sensor networks in a broad range of applications. Health, military, and home are some of the application fields. For example, the short deployment, self-running, and oddity tolerance features of military sensor networks make them a highly promising sensing strategy for military guidance, running, communications, computing, intensity, tracking, detection, and targeting systems. Sensor nodes may also be installed in the health sector to track patients and support disabled patients. Managing inventory, tracking product quality, and monitoring disaster zones include several other commercial applications. Wireless ad hoc networking techniques are important for the realization of these and other sensor network applications. Although several protocols and algorithms have been suggested for respected ad hoc wireless networks, they are not neatly tailored to the sensor networks' specific features and application requirements.

Security Requirements

There are very different wireless sensor networks from other wireless and wired networks. In wireless communication, protection is very critical as sensor nodes are so easily susceptible to various types of attacks and threats in real environments. Security is the primary focus for sensitive wireless sensor applications because node hacker installations target the sensory nodes in real environments and get access to the data or alter the real data with false data/wrong data to the base station for false environmental data analysis.

Data Confidentiality

Data confidentiality is a crucial part of the wireless sensor network. The data that passes through the network must be confidential. To ensure data confidentiality, sensor node information such as its sensor identities and public keys should be protected using distinct algorithms such as cryptography. Sensor nodes exchange very sensitive data so that their privacy is very important; the sensor network does not leak to the neighboring networks its sensor readings. The standard approach to data encryption is to encrypt confidential data so that information can only be accessed by intended users.

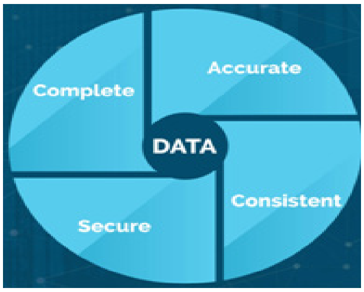


Data Authentication

In many administrative tasks, such as sensor reprogramming and sensor node duty cycle control, authentication is necessary. An adversary can inject messages to any sensor node so that it is authenticated by the sensor node whether or not it is the right source. Various authentication methods ensure that the sender node is authenticated, such as digital signature and cryptography.

Data Integrity

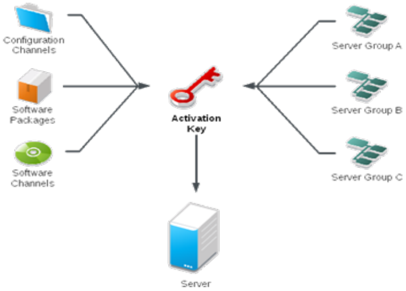
As sensor network data may be altered by compromise nodes, integrity controls must ensure that the obtained data is not altered before it reaches its original destination. Using a malicious node, the opponent can alter the data and alter the packet data before its destination and can give the receiver false information.



Group Key Management (GKM)

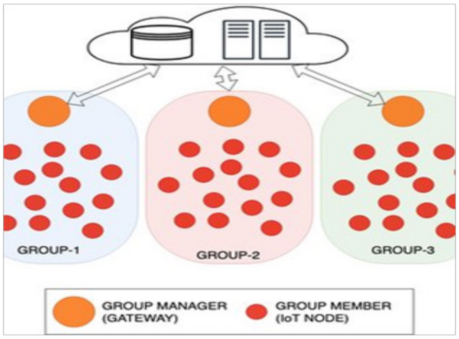
The essential security function provided by SGC is the provision of a common key, often known as the community key. The shared group key is used to encrypt and sign group communications, authenticate members and messages, and allow access to traffic and group resources. As a result, the most significant parts of SGC are the cryptographic strength of the keys and the key management protocol. Any stable group communication system should include a GKM system that satisfies the following criteria.

- Key generation is secure.
- Imitation of the group key should be infeasible or computationally difficult.
- The group key is securely distributed, and only the legitimate users can receive a valid group key.
- Revocation of the group key upon every membership change should be immediate.
- Every membership change must result in rekeying of associated keys.
- A rekeying of the key is secure.



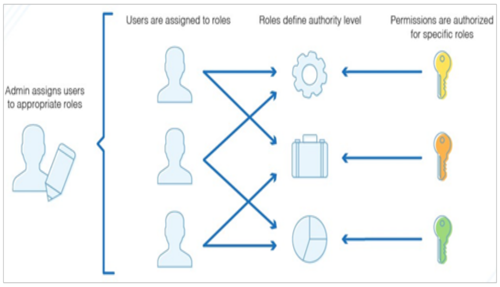
Group Authentication

A member of a group contact might be the designated sender, recipient, or both (one-to-many and many-to-many). To prevent identity-related threats, both users and communications should be verified. A trustworthy issuing entity certificate shall issue the Member Certificate in specific schemes, along with its validity time. The expired certificate is preserved in some schemes for further verification. Expired credentials are compiled into a circulating register of revocations to notify all participants.



Group Authorization and Access Control

In any classical access control method, a member who possesses a decrypting key may access the whole content (or all flows in an aggregated stream). This is known as a single right of the entrance. Multiple access privileges can be assigned to group members in a variety of community-oriented applications. As a result, a stream with varying access privileges should be accessed so that only members with an appropriate privilege may view the appropriate sections of the information (or flows). This is known as the right to numerous entries.

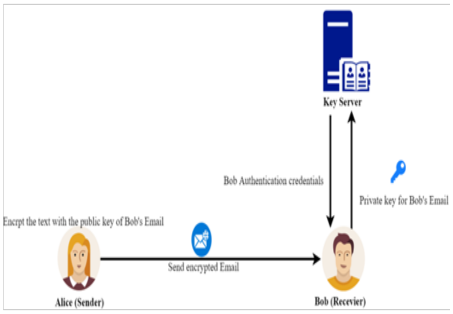

Users are assigned to roles
Roles define authority level
Permissions are authorized for specific roles
Admin assigns users to appropriate roles

Group Accounting and Nonrepudiation

Any community activity undertaken or a record of resources utilized by a participant should be available to monitor any abusive use of resources and activities. A non-repudiation service can ensure that the appointed authority can identify a participant whose activities are at issue in full and explicitly. In most cases, the community signature and member certificate may be used to verify the source and message, as well as offer proof of the source's operation in the event of a disagreement.

Group Privacy and Anonymity

To protect members' privacy and confidentiality, all information connected to group communication, such as the identity of the sender and receiver, as well as the duration and time of the communication, may be protected or disguised. Anonymous communication does not include the sender's or receiver's personal information.


Key Server
Bob Authentication credentials
Private key for Bob's Email
Encrpt the text with the public key of Bob's Email
Send encrypted Email
Alice (Sender)
Bob (Receivier)

Security Requirements in Secure Sensor Network

While various additional criteria are required for sensor network security, the fundamental criteria for WSNs listed above may not be adequate for sensor security. These are the requirements:

Data Freshness

The freshness of data The data in the sensor network is recent and does not replay (repeated packet) because the opponent can jam the network by compromising nodes or sending the same data packet through the network nodes to deplete the energy of the sensor nodes, which means that a specific node sends the same data packet due to a malicious attack that depletes the energy of the nodes and destroys the node. The ability to order is also ensured by the freshness of the data. Various security procedures are developed to guarantee that the data is fresh and simply delete it if it is a duplicated data node to prevent JAMMING in the network. The important institution ensures that the session is fresh. In essence, it is both a weak and strong key for data freshness preservation. There is partial but no delay information in weak packet ordering. Sensor readings and strong freshness are utilized to offer ordering facilities on request-response pairs and provide delay estimations required for network time synchronization.

Self Organization

Ad hoc networks are WSNs because they lack a stable infrastructure. Sensor nodes must be autonomous and flexible enough to be self-organizing and self-healing under many situations since once deployed in the sensor network; we cannot manually organize nodes in any condition, such as in the case of satellites. As a result, sensor nodes must be self-organized based on safe key management nodes to determine their location in the network via nearby nodes or GPS (global positioning system). After any node in the network fails, the new node will replace the failed node through a self-organizing method, ensuring that the network does not fail.

Scalability

For large or densely distributed networks, the number of sensor nodes ranges between 10 and 10,000. In such a huge network, only a few nodes have the power or resources to transmit data. When a node fails, all other network nodes are handled by replacement nodes, and key management can handle network scalability. In distributed sensor networks, key management is accomplished by segmenting the larger network into subgroups. When these subgroups are sent to another party, protection is given by re-encrypting messages. This technique is beneficial when the cost of transmission energy exceeds the cost of calculation.

Availability

The availability of nodes indicates the life lifetime of nodes. Sensor nodes should be protected from idle listening or excessive processing to maintain network node availability. Various routing protocols (LEACH, SPIN, GEAR, PEGASIS, HEED) are utilized to save energy and extend the network's life.

Time Synchronization

The majority of sensor network applications rely on some type of time synchronization. To save power, each sensor's radio can be turned off for short periods. Furthermore, sensors may desire to assess the end-to-end latency as it travels between two pair-wise sensors. A more collaborative sensor network can include group synchronization, etc., for monitoring applications. Provides a collection of safe synchronization protocols for sender-receiver (in pairs), multi-hop sender-receiver (for use when the pair of nodes is not within the single-hop range), and group synchronization.

Accessibility

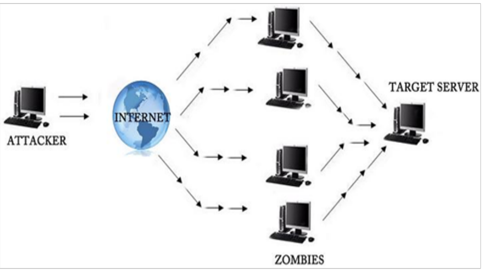
The key management system must grant access to intermediary nodes. Data fusion by each sensor node may be avoided if node-to-node secrecy is guaranteed since each node in its network receives the sensor data of another node via some key-specified method, such as direct or transitive key management systems. In the case of a direct key, all sensor network nodes share a single network key. Each node has a distinct key to decrypt/verify the data collected and another key to re-encrypt the data before it is transmitted to the next node in the transitive key management scheme. This main mechanism is utilized for small gatherings.

Types of Attacks

Data Integrity and Confidentiality-Related Attacks

Denial of Service on sensing (DoSS) attack

An intruder tampers with data until sensor nodes read it, resulting in erroneous readings and, eventually, a bad judgment. A DoSS attack often targets physical layer applications in an area where sensor nodes are situated.



Buffer Overflow Attack

The most common catch-all term for DoS assaults that deliver more traffic to a network resource than the engineers who developed the resource ever imagined. One such assault provided files with 256-character file names as email attachments to users using Netscape or Microsoft email clients; longer-than-expected file names were enough to crash such apps.

DDoS Attack

The attacker can employ PCs or other network-connected devices that have been infected with malware and have become part of a botnet. Distributed denial-of-service attacks, particularly those involving botnets, employ command-and-control (C&C) servers to direct the operations of botnet members. The command and control servers select the sort of attack to be carried out, the sorts of data to be communicated, and the targeting of networks or network resources in the assault.

Ping-of-death Attack

The Packet Inter-Network Groper (ping) protocol is misused by sending request messages with enormous payloads, causing targeted systems to become overloaded, avoiding responding to genuine requests for service, and potentially crashing the victim systems.

SYN Flooding Attack

TCP breaches the handshake protocol, which a client uses to establish a TCP connection with a server. The attacker sends a high-volume stream of requests to open TCP connections to the target server in an SYN flooding attack, with no intention of actually completing the circuits. The cost of establishing the SYN request stream is very minimal, but responding to such queries is resource-intensive for the victim. As a result, a successful attacker can deny genuine users access to the targeted server.

Teardrop Attack

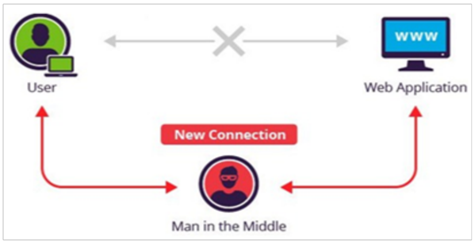
It makes use of flaws in how older operating systems handle fragmented Internet Protocol (IP) packets. When packets get too large for intermediary routers to process, the IP design allows for packet fragmentation and requires packet fragments to indicate fragment offsets; fragment offsets are adjusted to overlap with one other in teardrop assaults. The pieces may not be reassembled by hosts running impacted operating systems, and the assault may potentially cause the device to crash.

Node Capture Attack

An attacker physically captures and exploits sensor nodes, causing sensor readings from compromised nodes to be faulty or manipulated. The intruder can also obtain essential cryptographic keys (e.g., a group key) from wireless nodes, which are used to protect communications in most wireless networks.

Eavesdropping Attack

An attacker discreetly listens to ongoing communications between targeted nodes to gather connection information (e.g., medium access control [MAC] address) and cryptography (e.g., session key materials). Although this assault can be classified as another type, such as a privacy-related assault, we classify it as a cryptographic assault. The cryptographic information acquired may crack the encryption keys, allowing the attacker to extract significant data.



Power Consumption Related Attacks

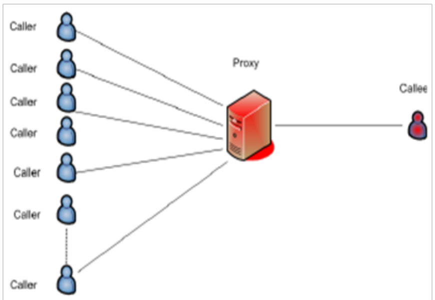
Denial of Sleep Attack

An attacker attempts to drain a wireless device's limited power source (particularly sensor devices) to severely reduce the node's lifespan. In general, the MAC layer protocol minimizes node power consumption by restricting radio communications during a sleep period when no radio transmission occurs. As a result, the attacker targets the MAC layer protocol to reduce or deactivate the sleep cycle. If the number of power-drained nodes is large enough, the entire sensor network can be severely affected.

Service Availability and Bandwidth Consumption Related Attacks

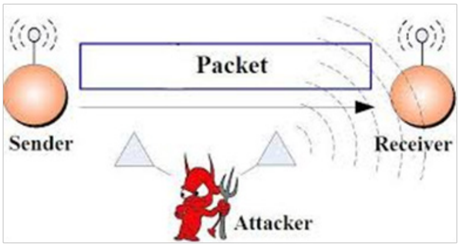
Flooding Attack

An attacker often sends a huge quantity of packets to the access point or a victim to prevent the victim or the whole network from creating or sustaining connections.



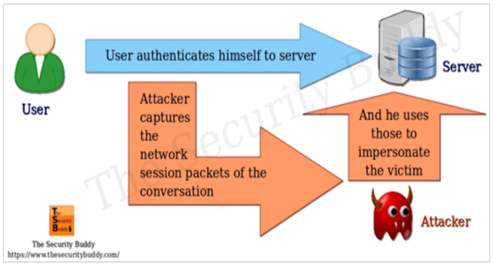
Jamming (Radio Interference) Attack

An attacker can successfully block off the wireless connection between nodes by broadcasting continuous radio signals that deny other authorized users access to a given frequency channel. The attacker may also emit jamming radio signals to purposefully collide with genuine signals provided by target nodes.



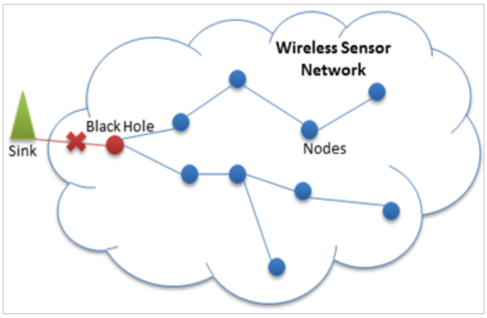
Replay Attack

An attacker replicates a forwarded packet and then transmits the duplicates repeatedly and continuously to the victim to overwhelm the victim's buffers or power sources or to base stations and access points on degrading network output. Furthermore, in poorly built devices, replayed packets might cause apps to crash or exploit susceptible gaps.


User
User authenticates himself to server
Server
Attacker captures the network session packets of the conversation
And he uses those to impersonate the victim
Attacker
The Security Buddy
https://www.thesecuritybuddy.com/

Selective Forwarding Attack

A forwarding node selectively ignores packets generated or forwarded by other nodes and instead forwards other unrelated packets.



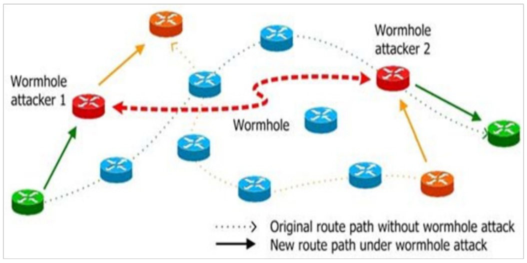
Routing Related Attacks

Unauthorized Routing Update Attack

An intruder attempts to update routing information stored by routing hosts, such as base stations, access points, or nodes for data aggregation, by exploiting routing protocols, forging messages for routing updates, and wrongly updating the routing table. Many events can occur as a result of this assault, including some nodes being detached from base stations; a network being partitioned; messages being routed in a loop and lost after the time to live has expired (TTL); communications are sent to unauthorized attackers inadvertently; a black-hole route is constructed in which messages are deliberately destroyed; and a prior key is still utilized by present members because false routings misroute or postpone rekeying communications designated for members.

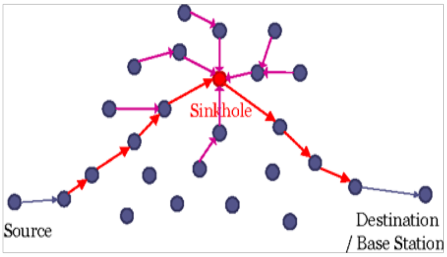
Wormhole Attack

An opponent intercepts the sender's communications, copies a portion of the entire packet, and accelerates the transmission of the copied packet through a custom wormhole tunnel, causing the duplicated packet to reach the destination quicker than the original packet did over normal channels. Several transmissions across a wireless channel through a wired network can be used to form a wormhole tunnel, and at the end of the tunnel, employing a long-distance boosting antenna, transmitting over a low-latency link, or utilizing any out-of-bound channel The wormhole attack poses numerous threats, particularly to routing protocols and other protocols that rely heavily on geographical location and proximity, and once the wormhole route has attracted a large number of traversing packets, a variety of subsequent attacks (e.g., selectively forwarding, sinkhole) can be launched. Readers are referred to for information and a way to identify such an attack.


Wormhole attacker 1
Wormhole attacker 2
Wormhole
Original route path without wormhole attack
New route path under wormhole attack

Sinkhole Attack

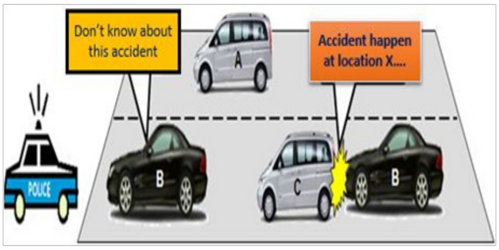
An attacker induces all nodes to pass all packets through one or more of its colluding nodes, known as sinkhole nodes, such that the attacker (and its colluding group) has access to all packets that are traversed. The sinkhole node is often considered as an alluring forwarding node to recruit victims nodes, such as having a greater degree of confidence, being advertised as a node at the shortest distance or with the lowest latency path to a base station, or being advertised as the nearest data aggregation node (in WSNs).



Identity-Related Attacks

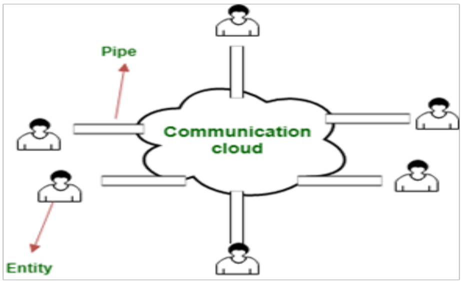
Impersonate Attack

An attacker impersonates the identity of another node (either MAC or IP address) to connect to or launch other attacks on a victim; the attacker can also exploit the victim's identity to connect to or launch other attacks on the victim's behalf, as shown in Fig. 1. Some programs are capable of reprogramming devices to fabricate MAC and network addresses.


Don't know about this accident
Accident happen at location X....
A
B
C
B
POLICE

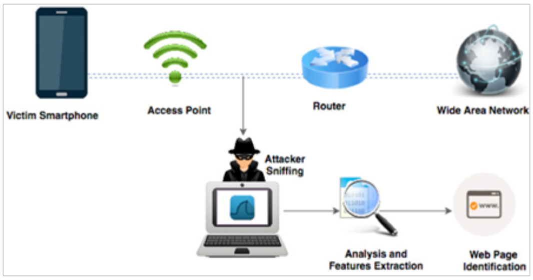
Sybil Attack

A single node sends messages to other nodes using faked IDs (either MAC or network addresses). The attacker may mimic the identities of other nodes or just create several arbitrary identities in the MAC and network layer. For example, packets traversing a route comprised of forged identities are deliberately discarded or changed, or a threshold-based signature method reliant on a predefined number of nodes is hacked. The attack then represents a hazard to further protocol levels.



Traffic Analysis Attack

An intruder tries to learn about the network's, traffic's, and nodes' behavior. Checking the length of the message, the pattern or coding of the message, and the time of the message remaining on the router are all examples of traffic analysis. Furthermore, the attacker will correlate all incoming and outgoing packets at all routers and participants. Because communications are linked to them, such an assault violates privacy and can potentially harm members (e.g., religious-related opinions that are deemed provocative in some communities). The attacker may perversely connect any two members with unconnected relationships.



Conclusion

Wireless sensor networks are being employed in a variety of applications as a result of their rapid growth. Security and dependability are hence the major concerns in every wireless sensor network application. This document reviews many sorts of conceivable network layer assaults and outlines feasible responses against them. Because wireless networks are more vulnerable to assaults, security measures must be powerful enough to prevent adversaries from affecting the network. It is required to handle data with total secrecy and high security, but because of its tiny battery capacity and restricted processing memory, it is restricted against large security algorithms. Thus it requires simple and effective approaches to ensure its security.

References

Abwao, V. *Information Technology Applications in Business Management within Kenyan Companies; A Survey of Selected Insurance Firms in Nairobi*. University of Nairobi, 2002.

Akyildiz, I.F., et al. "A Survey on Sensor Networks." *IEEE Communications Magazine*, vol. 40, no. 8, 2002, pp. 102-114.

Anwar, Raja Waseem, et al. "Security Issues and Attacks in Wireless Sensor Network." *World Applied Sciences Journal,* vol. 30, 2014.

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.

Davidescu, Andreea. "Virtual Enterprises Reach for Cloud Computing." *Journal of Mobile, Embedded and Distributed Systems*, vol. IV, no. 2, 2012, pp. 134-139.

Fajrin, Tina. "Analisis Sistem Penyimpanan Data Menggunakan Sistem Cloud Computing Studi Kasus SMK N 2 Karanganyar." *Indonesian Journal of Network & Security*, 2012.

Handayani, Putu Wuri, et al. "Mesin Pencari Berbasiskan Semantik Untuk Bahasa Indonesia." *Jurnal Sistem Informasi*, vol. 4, no. 2, 2012.

Kaur, Mandeep, et al. "RFID Technology Principles, Advantages, Limitations & Its Applications." *International Journal of Computer and Electrical Engineering*, vol. 3, no. 1, 2011, pp. 151-157.

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.

Modares, Hero, et al. "Overview of Security Issues in Wireless Sensor Networks." *International Conference on Computational Intelligence, Modelling & Simulation*, 2011.

Pathan, A.S.K., 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.

Purnamawati, Harnita Margareta. “Pelacakan Index Kata Universitas Pada Portal Mesin Pencari Studi Kasus: Universitas Area Kopertis 6 Jawa Tengah.” *Seruni,* 2012.

Rajasegarar, S., et al. “Anomaly Detection in Wireless Sensor Networks.” *IEEE Wireless Communications*, vol. 15, no. 4, 2008, pp. 34-40.

Ramon, Rodrigo, et al. “Situation Awareness Mechanisms for Wireless Sensor Networks.” *IEEE Communication 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.

Retnaningsih, Esti, and Bambang Eka Purnama. “Pelacakan Lokasi Hosting Web Perguruan Tinggi Studi Kasus: Perguruan Tinggi Kopertis 6 Jawa Tengah.” *Seruni*, 2012.

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.

Sriram, T., et al. “Applications of Barcode Technology in Automated Storage and Retrieval Systems.” *International Conference on Industrial Electronics, Control, and Instrumentation*, 1996.

Taqwa Hariguna, Berlilana. “Isu Cloud Computing e-government di Indonesia 2014.” *SNATIKA,* 2011.

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.

Zhou, Yun, et al. “Securing Wireless Sensor Networks: A Survey.” *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, 2008, pp. 6-28.

Author Details

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