



www.ijonest.net

Current Security Threats in Applications of Wireless Sensor Network

Ayuba John 

Universiti Teknologi Malaysia, Malaysia

Ismail Fauzi Isnin 

Universiti Teknologi Malaysia, Malaysia

Syed Hamid Hussain Madni 

Universiti Teknologi Malaysia, Malaysia

To cite this article:

John, A. Isnin, I. F., & Madni, S. H. H. (2023). Current security threats in applications of wireless sensor network. *International Journal on Engineering, Science, and Technology (IJONEST)*, 5(3), 255-272. <https://doi.org/10.46328/ijonest.174>

International Journal on Engineering, Science and Technology (IJONEST) is a peer-reviewed scholarly online journal. This article may be used for research, teaching, and private study purposes. Authors alone are responsible for the contents of their articles. The journal owns the copyright of the articles. The publisher shall not be liable for any loss, actions, claims, proceedings, demand, or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of the research material. All authors are requested to disclose any actual or potential conflict of interest including any financial, personal or other relationships with other people or organizations regarding the submitted work.



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

Current Security Threats in Applications of Wireless Sensor Network

Ayuba John, Ismail Fauzi Isnin, Syed Hamid Hussain Madni

Article Info

Article History

Received:

14 January 2023

Accepted:

19 May 2023

Keywords

Wireless sensor network

Security threats

Cyber security

Data integrity

Abstract

Wireless sensor networks have a broader application range in almost every field of human endeavours, which exposes them to a variety of security threats on a daily basis from cyber criminals. It is a remote monitoring system for events or phenomena in areas such as smart grids, intelligent healthcare, circular economies in smart cities, and underwater surveillance. Cybersecurity threats have long been a source of concern in the field of wireless sensor networks. The goal of cyber security in this era is to certify the authenticity of networks confidentiality, data integrity and availability of network assets. Various security mechanisms, particularly key management cryptographic, authentication mechanisms, and intrusion detection systems have been developed from several machine learning algorithms, and so on, which have been used to ensure network security. In this paper, we focused on outlining diverse application areas of wireless sensor networks with their security threats, major challenges and given some common mechanism to counter security threats for in-depth research insight on security in applications of wireless sensor networks. In addition, an analysis of the common attacks on wireless sensor networks has been provided.

Introduction

Wireless Sensor Networks (WSNs) are either homogeneous or heterogeneous, depending on whether the network is made up of distributed nodes with the same properties; independent, dynamic topology, energy conservative and mission-adopted wireless nodes, or nodes with different properties and abilities. Homogeneous WSNs applications do not rely on infrastructure installation to communicate, whereas heterogeneous WSNs applications do. One of the major challenges of WSNs however, is the security and accuracy of sensor nodes, Bhushan and Sahoo (2020).

The increasing use of wireless sensor networks in various fields of human endeavor has resulted in a slew of novel network attacks by cybercriminals, Alawida et al. (2022). With the wide range of wireless sensor network applications in almost every field of human endeavours, particularly smart grids, intelligent based healthcare, big data environment, circular economy in smart cities, underwater creature and tactical surveillance, smart green data gathering with cloud, Ad-hoc sensor networks, global internet of things, and the oil and gas industry where security threats have been the most serious issue, Kraidi et al. (2019).

Wireless Sensor Networks have many advantages and they are also vulnerable to a variety of security threats, Bhushan and Sahoo (2018). In the context of WSNs, the terms "attacks" and "threats" are frequently used interchangeably, though they refer to different concepts, Liu and Labeau (2021). The primary distinction between threats and attacks in WSNs is that threats are potential dangers, whereas attacks are actual malicious acts aimed at exploiting network vulnerabilities, Tsiknas et al. (2021). Various security techniques, such as encryption, secure key management, secure routing, and intrusion detection and prevention, have been proposed to prevent these security threats, Khan et al. (2020). These techniques can help to improve the security of communication and data transmission in wireless sensor networks.

Security threats in a WSN are those that interfere with or disrupt network information confidentiality, integrity, and availability, Alkudhayr et al. (2019). However, confidentiality ensures that sensitive information transmitted over the network is protected from unauthorized access. Integrity ensures that data transmitted over the network is not altered. Availability ensures that the network and data communication are always available even when there are attacks.

The remaining sections of the paper is organised as follows: Section 2 reviews related work, Section 3 describes security in WSNs, Section 4 discusses several security threats in WSN applications, Section 5 discuss common security threats in WSNs, and Section 6 describes the security mechanism to counter attacks in WSNs.

Review of Related Works

By integrating packet radio service and radio frequency identification and achieving good data aggregation transmission monitoring, Zhu (2021) proposed an energy calculation method for direct transmission and a low energy multiple-hop route protocol to solve the problem of energy imbalance for energy depletion attacks in fusion wireless sensor networks. The research by Kuthadi et al. (2022), have introduced manageable and tolerance data security for denial of service (DoS) attacks in wsn, as well as modelled an effective energy frame-work for detecting anti-node development collection in anticipation for excellent data security and network management in order to reduce the rate of energy utilization in a smart grid location.

Anitha et al. (2021), has attempted to address the issue of node compromise attacks that lead to node replication in intelligent-based healthcare systems by using an average exponential affecting imitation detection and secured ant colony optimization, which yielded a better detection probability.

Panahi and Bayılmış (2022), used reserved bits in the MAC header ZigBee to choose between insecure and secure modes and provided an alternative security means using fantomas and camellia algorithms to reduce bit error rate during data transmission in a big data environment. Liu et al. (2022a), proposed an entropy-based topology control strategy that maintains required topology connectivity for each node to prevent underwater spy-robots from hacking into the wsn to eavesdrop useful data information and contaminate some nodes with viruses.

In a smart green data gathering with cloud, Boukerche et al. (2006) proposed a periodic event-driven and query-

based protocol to provide low latency and high reliability for packet delivery, as well as a cluster-based routing protocol to group sensor nodes and reduce high network data traffic. Barati (2022), introduced hierarchical key management to provide security against eavesdropping attacks, albeit at a higher network overhead. Lin et al. (2022), proposed an algorithm for anomalous prediction in network security on cloud computing to overcome the security risk of data in flowmeter for multi-sensor data fusion workstation.

Halle and Shiyamala (2022), introduced a novel secure and dependable advanced metering infrastructure protocol based on lightweight cryptographic techniques with integrated elliptic curve cryptography for data integrity. Haseeb et al. (2022), proposed an energy-efficient routing protocol and integrated an international data encryption algorithm based on symmetric-key block cyphers for mobile node ad-hoc sensor networks to protect data from threats. In this research paper, we have identified a number of critical areas of wireless sensor network applications in the advancement of technology in human endeavours, malicious threats of various types have been identified in wireless sensor network applications and have provides several counter-approaches to security threats in WSN applications.

Security in Wireless Sensor Networks

In network security configuration, a firewall cannot be used interchangeably as an Intrusion Detection System (IDS) or as a cryptography technique. They both have opposing viewpoints and approaches to network security. The firewall can act as a defender against an external attacker by limiting and preventing access to the network, but it cannot detect anomalous activity that originates within the network, none of the cryptographic techniques can handle it. IDS can detect and evaluate any suspicious network activity and raise a flag to alert the human analyst to take appropriate action on the intruder or anomaly packet. Figure 1 depicts an overviews of security diversity in wireless sensor networks.

Security in wireless sensor networks is divided into three study areas in Figure 1: security threats, security mechanisms, and security class. Wireless sensor network security aims to provide confidentiality, ensure data integrity, and ensure the availability of network system information against any type of threat or malicious attack that attempts to gain unauthorized access into the system in order to steal or damage vital information.

The security mechanisms are the devices that can be used to prevent or detect any security threats from disrupting the normal operation of the network services through any form of security class such as interruption, interception, modification, or fabrication of the network parameters.

The focus of the main research work is on the security mechanism by which a network intrusion detection system is considered a high-level mechanism that could be used in a heterogeneous cluster-based wireless sensor network. However, in this paper, the focus is on identifying several types of malicious threats in the network traffic and intruders in the networks that cannot be identified by a network firewall or by cryptographic techniques.

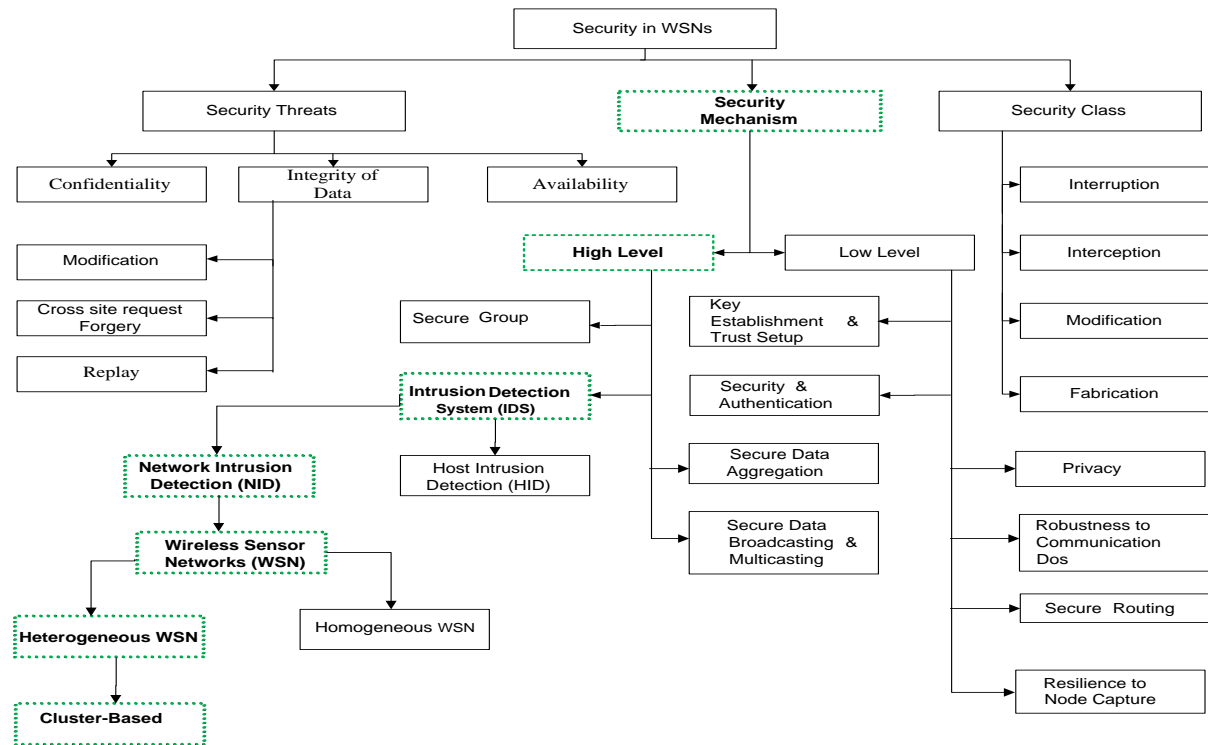


Figure 1. The Overviews of Security Diversity in Wireless Sensor Networks

Security Threats in Wireless Sensor Networks

In industry and agriculture, WSNs have variety of applications specially to collect environmental data, track animal footprints, analyse pollution situations, predict the spread of forest fires, and create intelligent debris flow products, John and Igimoh (2017). In hospitals WSN collect physiological data from patients, analyse their conditions, and provide timely medical healthcare for patients, Huanan et al. (2021).

The performance of WSNs is of a critical important in the automation process, necessitating low complexity, light weight, and high security mechanisms for anomaly detection and authentication. As a result, security is critical in the WSNs used in industries to protect the engineering operation system from being disrupted by an attacker's malicious nodes, which can disrupt the production process and cause unpredictability in economic losses, Ghoreishi and Isnin (2019). The following are the numerous applications of wireless sensor network and the security challenges they present:

Attacks on Wireless Sensor Networks in Smart Grids

Recent machine-to-machine data security issues on the smart grid are discussed, as are available solutions for detecting and avoiding cyber threats, Almasarani and Majid (2021). For WSN-based monitoring systems in the electrical power grid as shown in Figure 2, data is collected in real time from several sensor nodes installed in the smart grid. Simple spear phishing, snooping, re - transmission, packet analysis, man-in-the-middle attacks, halting, and more complex route discovery attacks are all possible, making these sensors vulnerable to a wide range of cyber security threats (Sybil threats, selective forwarding, and hello floods). The threats are carried out on various

layers of WSNs, such as jamming and hacking, which are physical layer attacks aimed at data tampering, sensor node position modification, and the introduction of fraudulent nodes into the network.

Spoofing attacks are directed at the data link layer, which is in charge of logical link control and media access control. The Sybil attack, which isolates nodes by modifying the routing to cause the node to report false identities in order to destroy a network, is a common form of network-layer denial-of-service (DoS) attack.

The flooding attacks on the transport layer can render network resources unavailable. When smart grid infrastructures are vulnerable to cyberattacks, the complex architectures and communication systems they use can result in deficits in national security, disruptions in public order, loss of life, or widespread economic harm, Gunduz and Das (2020).

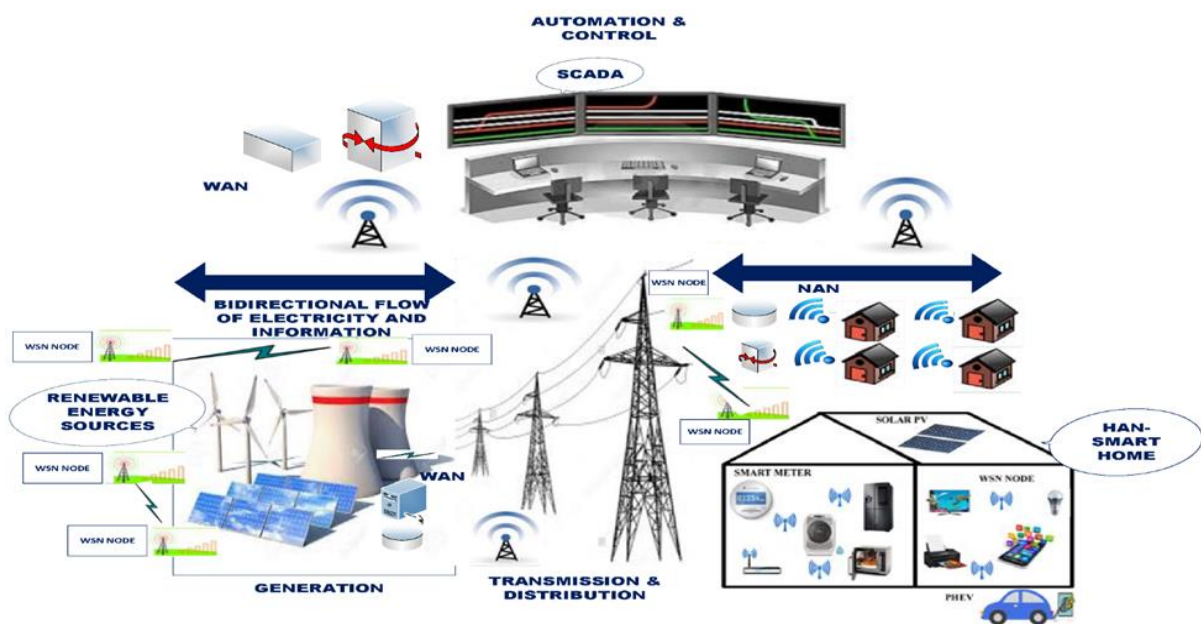


Figure 2. Wireless Sensor Networks in Smart Grids, Chhaya et al. (2017)

Attacks on Intelligent Based Healthcare Security Monitoring

The impact of WSN at various levels in healthcare monitoring systems, including the hardware layer and unrelated flaws, raises the prospect of future threats and data breaches. As their target, cybercriminals launch a variety of attacks on the gateways connected to the WSNs. The node compromise attack, which may result in a node replication attack, is the most common type of attack launched by attackers. In contrast, a security mechanism can be used in the intelligent healthcare monitoring system to detect and protect against attacks, Anitha et al. (2021).

Mostly static WSN is used in healthcare application systems such as daily routine activity monitoring, Remote real-time motion detection, location tracking, and prescription dosage tracking as shown in Figure 3. However, because the system is susceptible to a variety of cyber threats, including both passive and active threats multi-level security must be implemented across all network segments to prevent such attacks.

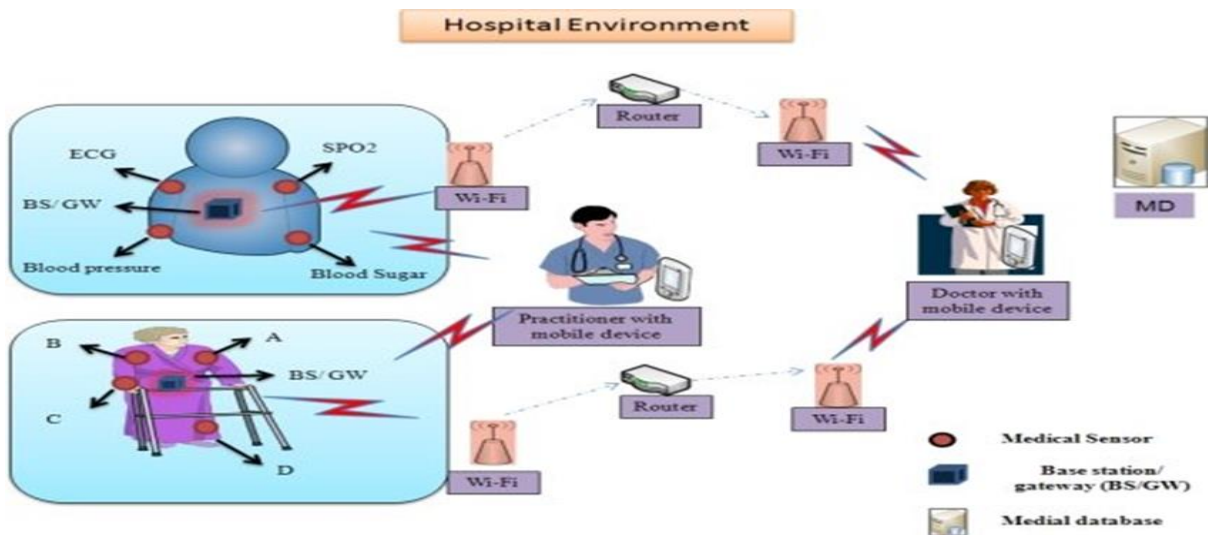


Figure 3. Intelligent based healthcare security monitoring, Kumar et al. (2012)

Attacks on Wireless Sensor Networks in Big Data Environment

The data capture and access process are critical in big data applications, but it has a number of security flaws. An attacker could exploit such flaws to compromise user privacy, maintain sensor node confidentiality and regulate the channel of communication among networking devices; thus, WSN authentication is a critical concern. WSNs, which typically the vast majority of big data applications rely on a huge number of sensor nodes of limited computational capabilities, Nashwan (2021). Big data in WSNs necessitates users collecting data in real time from sensor nodes within the same communication range as shown in Figure 4, while transmission channels between authentication entities within the envisioned location are unreliable, all verification information can be intercepted, deleted, captured, modified, and retransmitted by an intruder.

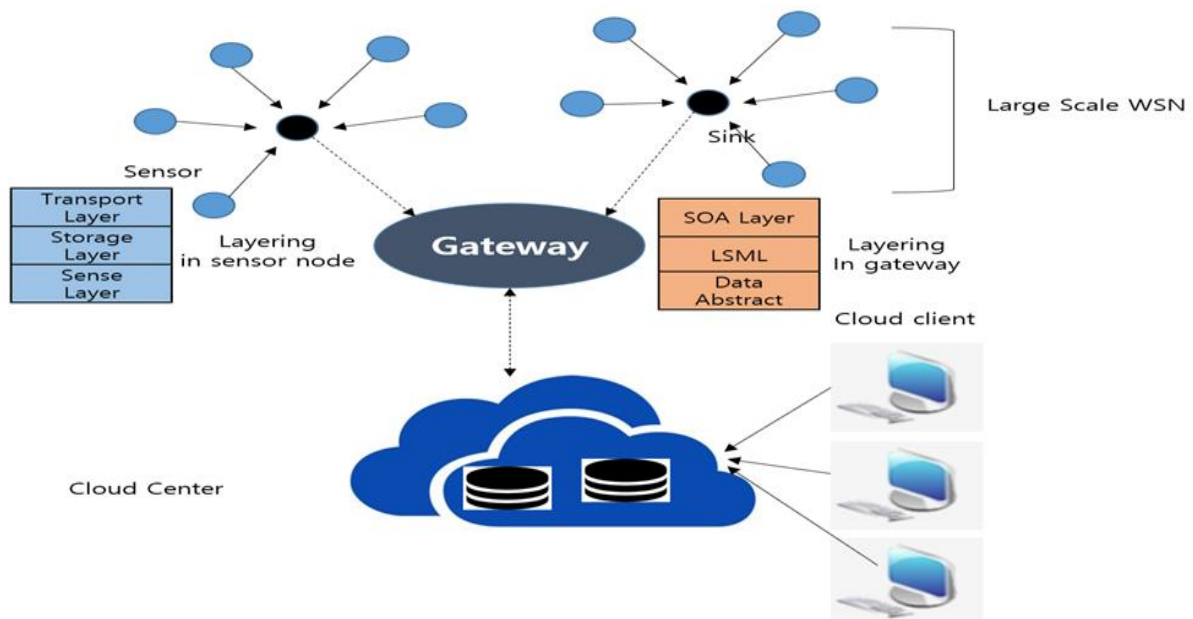


Figure 4. Wireless Sensor Networks in Big Data Environment, Kim et al. (2019)

Attacks on Circular Economy in Smart Cities

A smart city is a community which consolidates innovative wearable technologies, data, and technology communication to help cities manage their assets more effectively, Li et al. (2021). Smart cities use WSNs to identify, compute, evaluate, and monitors to improve environmental components in medical care, transportation, agriculture, industrial process control, and economic growth as shown in Figure 5. They provide, among other things, smart home, smart energy, smart lives, smart driving, smart health, and smart management. Smart city sensor nodes are vulnerable to cyber-attacks and must be properly secured. Although many lightweight authentication mechanisms have been developed to achieve secure communication in real-time applications, Because of the lack of synchronization between nodes during data routing, WSNs are extremely susceptible to DoS attack, Premkumar and Sundararajan (2020).

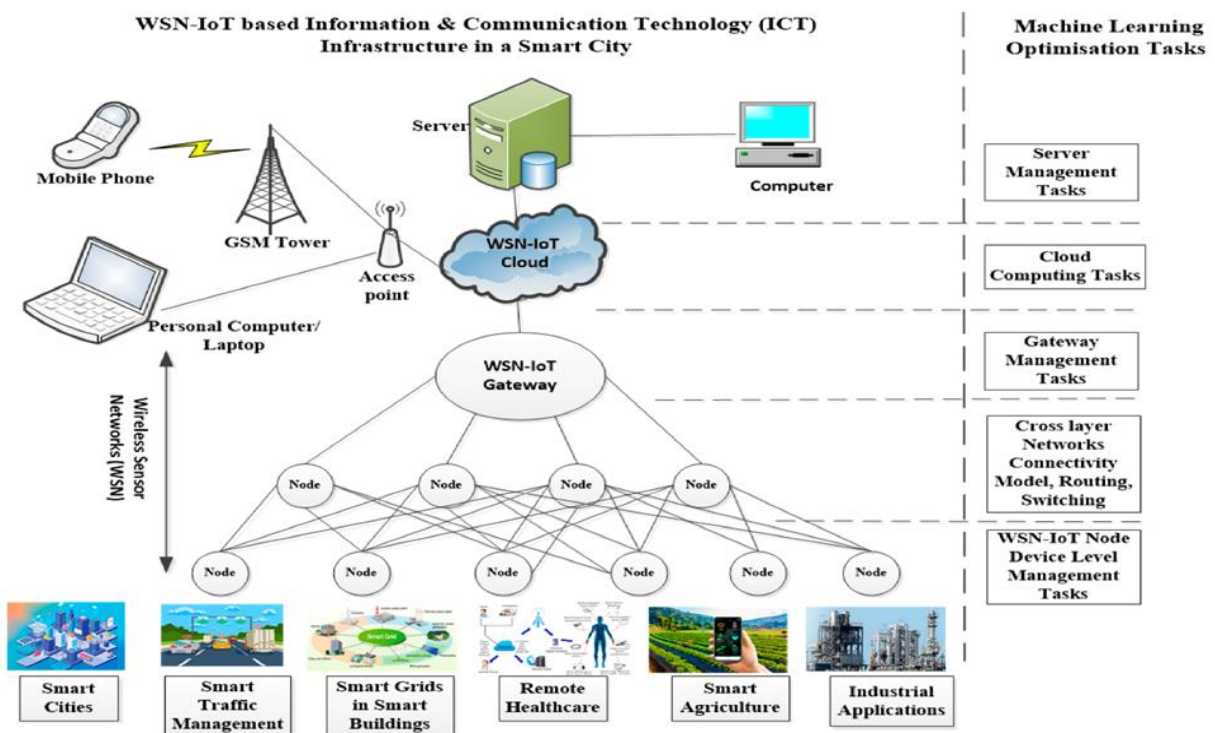


Figure 5. Circular Economy in Smart Cities Sharma et al. (2021)

Attacks on Underwater Creature Tracking and Tactical Surveillance

Underwater spy robots as shown in Figure 6, acting as eavesdroppers or hackers could compromise underwater acoustic sensor networks, particularly those used in military applications, Liu et al. (2022b). The data messages could contain sensitive information, particularly about undersea tactical environments, and the adversary could send spy robots to invade and snip data messages, or virus-infect wireless sensor network nodes. Data theft and cascading failures are two common security threats. Thus, data theft occurs when underwater spy robots start moving across connected nodes and listen in on their messaging services, whereas cascading failures occur when hackers masquerade as normal nodes and spread the virus the connected nodes.

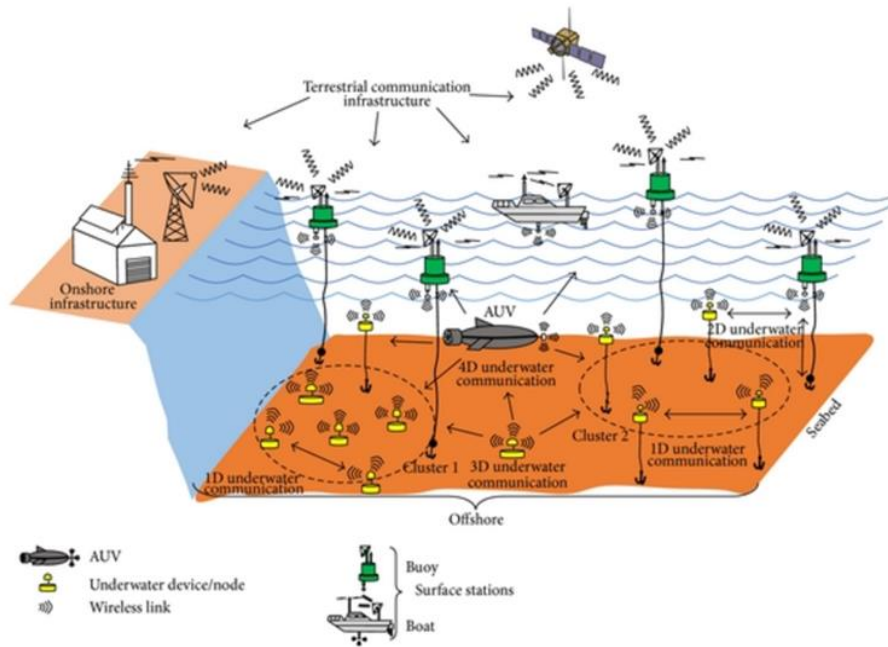


Figure 6. Underwater creature tracking and tactical surveillance, Felemban et al. (2015)

Attacks on Smart Green Data Gathering with Cloud

Because of the more flexible and changeable infrastructure, attacks and unidentified nodes can easily infiltrate mobile wireless sensor networks, putting data security at risk and destroying or altering private information regarding smart green application domains, Haseeb et al. (2022). However, because of sensor node-bound constraints and accessibility, the vulnerability of data inaccuracy and disaster is frequently extremely high, especially with large-scale smart green application areas as shown in Figure 7.

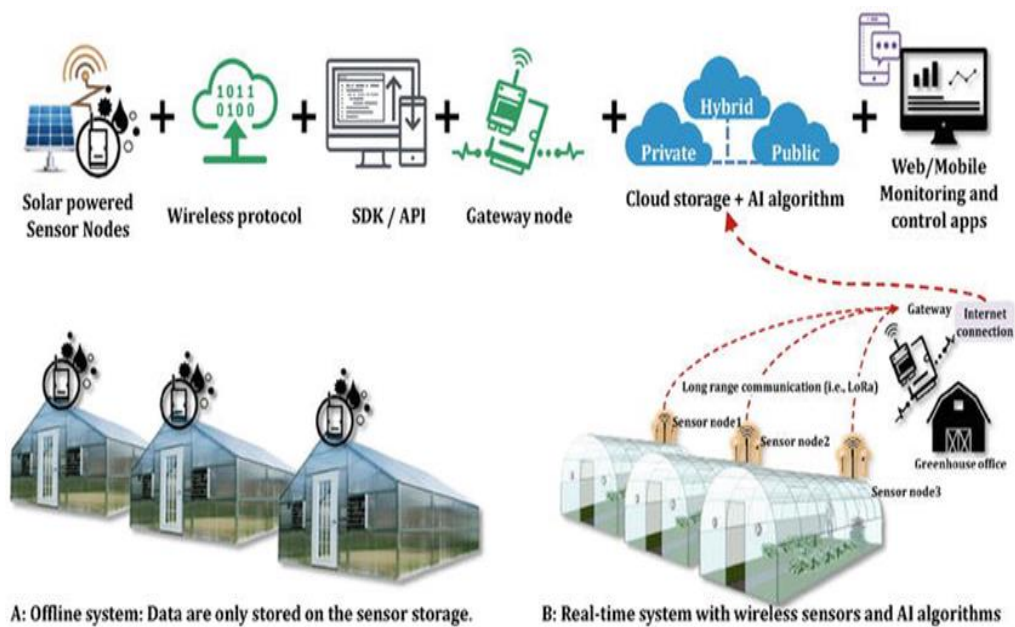


Figure 7. Smart Green Data Gathering with Cloud, Shamshiri et al. (2021)

Attacks on Wireless Ad-hoc Sensor Networks

Wireless Ad-hoc Networks as shown in Figure 8, are vulnerable to revolving and stretch attacks that cause DoS due to the unsupervised nature and deployment of wireless sensors in challenging situations such as border security, healthcare and defense, Jasper (2021).

Hackers can introduce suspect data into the network via malicious node, causing the base station to make incorrect decisions and reducing the network's lifespan. If the compromised nodes are not discovered, more false data may be injected into the sink, causing DoS. An attacker can obtain sensitive information shared by the nodes and disable the network, or they can conduct attacks like black hole attack, vampire attacks, and crosstalk attacks, which can drain battery resources by sending malicious data chunks to sensor nodes.

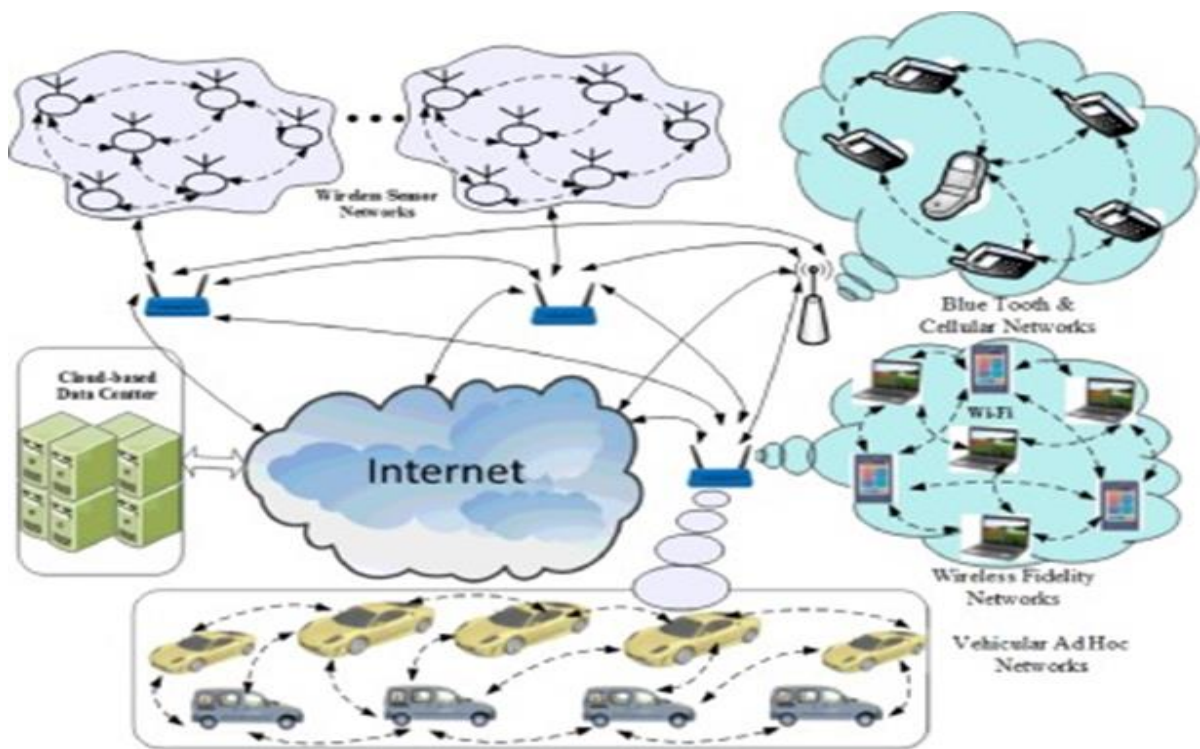


Figure 8. Wireless Ad-hoc Sensor Networks Qiu et al. (2017)

Attacks on Global Internet of Things Framework

A user may request delicate data generated by asset smart sensors in network controlled by conceptual model nodes as shown in Figure 9.

The main concern with internet of things (IoT)-based applications, particularly those based on heterogeneous wireless sensor networks, is their susceptibility to malicious attack, Santos-González et al. (2020). Although secure encryption security can be used to control transmissions on internet modules and less restricted devices using handshakes and stately connections, the cost of securing restricted internet of things devices can have a significant impact on their effectiveness.

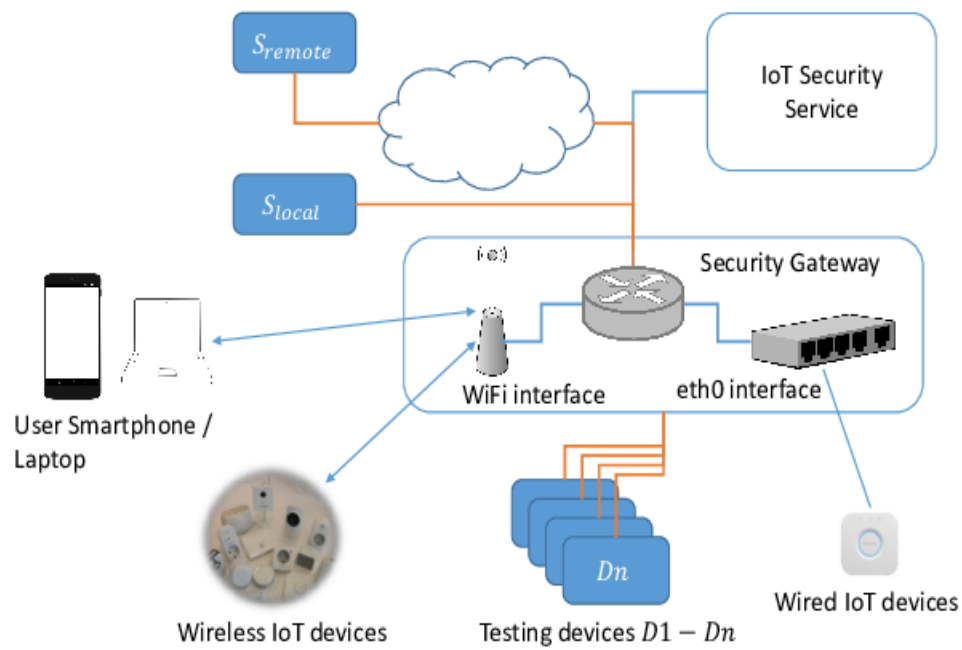


Figure 9. Global Internet of Things Framework, Miettinen et al. (2017)

Attacks on Real-time Monitoring in Oil and Gas Industry

In the oil and gas industry, WSNs are used for real-time production monitoring or well monitoring, and they can also be used for tracking as shown in Figure 10.



Figure 10. Real Time Monitoring in Oil and Gas Industry, Sundaram (2019)

Routing attacks in the sensor networks layer, which occur by routing information that is spoofed, altered, and replayed or by creating routing loops and extending service routes; sinkhole attacks, which occur by attracting a traffic packet flow; selective forwarding by a malicious node; sybill attacks by duplicating a node in multiple locations; wormhole attacks by recording and replaying a malicious packet, and A denial of service (DoS) attack occurs as a result of node failure or malicious action, Alam and De (2014). Denial of service attacks, such as jamming attacks that interfere with radio frequencies, tampering attacks that alter or replace nodes, collision attacks that cause multiple nodes to transmit packets at the same frequency at the same time, exhaustion attacks that cause repeated collisions, flooding attacks that repeatedly make new connection requests or cause desynchronization to disrupt an existing connection, are all threats that the network is vulnerable to as new threats emerge.

Common Attacks in Wireless Sensor Network

When the network system is used, it is targeted by two types of attackers: authorized users and legitimate users who have exceeded their legitimate boundaries. The second type of user is an illegal user, who attempts to gain unauthorized access to the network system in order to operate or attack critical network components, Zhang et al. (2022). Attacks on wireless sensor networks can take the form of either an active attack aimed at destroying network assets or a passive attack aimed at stealing valuable information from the networks. The following are some of the most common security threats in WSNs:

Sinkhole Attack: This is an attack in which an attacker manipulates network routing information to redirect traffic to a single malicious node, also known as a "sinkhole", Zaminkar and Fotohi (2020).

Eavesdropping: is the unauthorized interception of wireless signals. Eavesdropping in WSNs occurs when an attacker intercepts and listens to data transmitted between sensors and the base station, Rhim et al. (2020). This may jeopardize the confidentiality of the data being transmitted.

Malware attacks: are attacks that involve the deployment of malicious software in order to compromise system security and steal sensitive information, Ohm et al. (2020).

Tampering: is the unauthorized modification of data. In WSNs, an attacker can alter the data transmitted between sensors and the base station, Pruthi et al. (2019). This can jeopardize the integrity of the data being transmitted.

Phishing attacks: These are attacks that impersonate a trustworthy entity in order to trick users into providing their login credentials or sensitive information, Al-Hamar et al. (2021).

Wormhole Attack: This is an attack in which an attacker creates a virtual tunnel between two distant parts of the network in order to intercept and manipulate data transmission, Shahid et al. (2022).

Node Capture: it occurs when an attacker physically gains access to and controls a sensor node. Once an attacker gains control of a node, he or she can use it to launch attacks against other parts of the network, Alladi et al. (2020).

Clone of sensor nodes: The attacker replicates an original node by establishing a relationship that results in the capture of the original nodes' identities in order to create an exact replica of the sensor nodes, which are then deployed in the network at intelligently chosen locations by the attacker, Kulkarni et al. (2019).

Replay attacks: involve replaying captured packets in the network. This can lead to the network being

compromised or sensitive information being stolen, Iqbal and Mir (2022).

Physical threats: include natural disasters, equipment failures, and environmental factors that can compromise the network, Yaacoub et al. (2020).

Rushing attacks: involve quickly transmitting data across a network in order to exploit a vulnerability. As a result, the network may become overburdened and unavailable, Swessi and Idoudi (2022).

Insider threats: are the kind of attack prompted by employees or contractors with access to real-time monitoring systems. Insider threats could involve either intentional or unintentional system compromise, posing safety and security risks, Kim et al. (2020).

Sybil Attack: It is a type of attack in which an attacker creates multiple fake identities and uses them to gain control of parts of a network, Farjamnia et al. (2019). A Sybil attack can be used to disrupt the normal operation of a WSN.

DDoS attacks: These are attempts to flood the network with traffic, causing it to become unavailable. It has the potential to interfere with real-time monitoring of critical systems and operations, posing safety and security risks, Laaki et al. (2019).

Denial-of-Service (DoS) attacks: The primary goal of this type of attack is to disrupt all network services traffic flow to the target system and to prevent normal traffic from reaching the network by flooding the system with an abnormal amount of traffic after gaining access to the network, which the system cannot handle and instead shuts down to protect itself, Diro and Chilamkurti (2018).

Probe attacks: During probing, attackers scan the network for vulnerabilities and attempt to gather any potentially relevant information within the network, such as personal information about clients or banking information, in order to later cause havoc on the system, Dixit and Silakari (2021).

User-to-Root (U2R) attacks: The threats started with an insider gaining unauthorized access to a typical user account on the system and exploiting some security faults to gain root access to the system, Xiong et al. (2018).

Remote-to-Local (R2L) attacks: A remote intrusion is a malicious attack designed to gain local access to a remote computer or computer network. The remote attack has no effect on the attacker's computer. Rather, the intruder will look for defects in the security software of a computer or network in order to gain remote access to the device or system. Remote attacks are frequently used to gain unauthorized access to or steal data from a network, as well as to introduce viruses and other malicious events, Dixit and Silakari (2021).

Table 1. Analysis of Common Attacks in Wireless Sensor Networks

S/N	Security Attacks	Security Class	Active Attack	Passive Attack
1	Sinkhole	Interception, Interruption, Modification and Fabrication	✓	
2	Eavesdropping	Interception		✓
3	Malware	Interception and Interruption		✓
4	Tampering	Interception and Modification	✓	
5	Phishing	Interception		✓
6	Wormhole	Fabrication and Modification	✓	
7	Node capture	Interception, Interruption, Modification and	✓	

		Fabrication	
8	Clone	Interception, Interruption, Modification and Fabrication	✓
9	Replay	Interception and Interruption	✓
10	Physical	Interception, Interruption, Modification and Fabrication	✓
11	Rushing	Interception and Interruption	✓
12	Insider	Interception, Interruption, Modification and Fabrication	✓
13	Sybil	Interception, Interruption, Modification and Fabrication	✓
14	Distributed Denial of Service (DDoS)	Interception, Interruption, Modification and Fabrication	✓
15	Denial of Service (DoS)	Interception, Interruption, Modification and Fabrication	✓
16	Probe	Interception	✓
17	User-to-Root (U2R)	Interception, Interruption, Modification and Fabrication	✓ ✓
18	Remote-to-Local (R2L)	Interception	✓

Mechanism for Countering Attacks in Wireless Sensor Network

Various security mechanisms for WSNs have been proposed to ensure secure communication and prevent unauthorized access to the network and its data.

Cryptographic Techniques: are the most commonly used security mechanisms in WSNs to protect the confidentiality, integrity, and authenticity of data transmitted over a network, these techniques employ encryption algorithms such as AES, DES, and RSA, William et al. (2022). Cryptographic techniques can be used to secure node communication and prevent unauthorized network access.

Key Management: is an important aspect of securing WSNs, the scheme must be able to securely distribute encryption keys among nodes and update them on a regular basis to prevent key compromise, Boubiche et al. (2021). Key management schemes for WSNs have been proposed, such as the Hierarchical Key Management Scheme (HKMS) and the Distributed Key Management Scheme (DKMS).

Authentication: is the process of verifying the identity of network node, Passwords, digital certificates, and biometrics are all methods of authentication. Authentication in WSNs is typically done with symmetric key algorithms like HMAC and digital signatures, Kumar, and Ray (2022).

Access Control: is the process of limiting access to resources based on a node's identity, and can be implemented in a variety of ways, including role-based access control and attribute-based access control, Rouhani et al. (2021). Access control in WSNs can be used to restrict access to sensitive information such as sensor readings.

Intrusion Detection and Response are security mechanisms used in WSNs to detect and respond to security threats. Intrusion detection systems (IDSs) detect security threats in real time, and intrusion response systems

(IRSSs) respond to these threats by isolating compromised nodes or disconnecting them from the network, Kholidy (2021).

Trust management: is the process of determining the level of trust among network nodes and is used in WSNs to prevent malicious nodes from communicating and to ensure that only trustworthy nodes can communicate, Yin and Li (2019).

Conclusion

In this research paper, we focused on outlining the various application areas of wireless sensor networks, as well as their security threats and major challenges, in order to provide in-depth research insight on security in WSN application areas. We discussed security threats and provided a general overview of the major challenges that wireless sensor networks face in their wide range of applications. A wireless sensor network attack is likely to jeopardize data authentication, availability, confidentiality, and integrity. The clone attack, in particular, which is accomplished by a compromised sensor node replicating itself with the same identity, may contain all of the credentials of the legitimate member in order to appear authentic, and can have access to network. In addition, an analysis of the common attacks on wireless sensor networks has been provided.

Recommendations

We recommend that researchers try to develop several security mechanisms using various methods to address the current security challenges in the areas of wireless sensor network applications to human endeavours.

Acknowledgement

The authors would like to express their gratitude to the Nigerian Petroleum Technology Development Fund (PTDF) for providing the scholar with a fully funded scholarship to pursue his studies in this field.

References

- Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T., & Ramachandran, V. (2021). Enterprise Credential Spear-phishing attack detection. *Computers & Electrical Engineering*, *94*, 107363.
- Alam, S., & De, D. (2014). Analysis of security threats in wireless sensor network. *arXiv preprint arXiv:1406.0298*.
- Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences*.
- Alkudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information security: A review of information security issues and techniques. 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS),
- Alladi, T., Chamola, V., Sikdar, B., & Choo, K.-K. R. (2020). Consumer IoT: Security vulnerability case studies

- and solutions. *IEEE Consumer Electronics Magazine*, 9(2), 17-25.
- Almasarani, A., & Majid, M. (2021). 5G-Wireless Sensor Networks for Smart Grid-Accelerating technology's progress and innovation in the Kingdom of Saudi Arabia. *Procedia Computer Science*, 182, 46-55.
- Anitha, S., Jayanthi, P., & Chandrasekaran, V. (2021). An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks. *Measurement*, 167, 108272.
- Barati, H. (2022). A hierarchical key management method for wireless sensor networks. *Microprocessors and Microsystems*, 104489.
- Bhushan, B., & Sahoo, G. (2018). Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. *Wireless Personal Communications*, 98, 2037-2077.
- Bhushan, B., & Sahoo, G. (2020). Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective. *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 683-713.
- Boubiche, D. E., Athmani, S., Boubiche, S., & Toral-Cruz, H. (2021). Cybersecurity issues in wireless sensor networks: current challenges and solutions. *Wireless Personal Communications*, 117, 177-213.
- Boukerche, A., Pazzi, R. W. N., & Araujo, R. B. (2006). Fault-tolerant wireless sensor network routing protocols for the supervision of context-aware physical environments. *Journal of Parallel and Distributed Computing*, 66(4), 586-599.
- Chhaya, L., Sharma, P., Bhagwatikar, G., & Kumar, A. (2017). Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control. *Electronics*, 6(1), 5.
- Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82, 761-768.
- Dixit, P., & Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. *Computer Science Review*, 39, 100317.
- Farjamnia, G., Gasimov, Y., & Kazimov, C. (2019). Review of the techniques against the wormhole attacks on wireless sensor networks. *Wireless Personal Communications*, 105, 1561-1584.
- Felemban, E., Shaikh, F. K., Qureshi, U. M., Sheikh, A. A., & Qaisar, S. B. (2015). Underwater sensor network applications: A comprehensive survey. *International Journal of Distributed Sensor Networks*, 11(11), 896832.
- Ghoreishi, S., & Isnin, I. F. B. Design and analyze the security of a novel provablysecure and efficient key-management cryptographic scheme appropriate for wireless sensor networks.
- Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 169, 107094.
- Halle, P. D., & Shiyamala, S. (2022). Secure Advance Metering Infrastructure Protocol for Smart Grid Power System Enabled by the Internet of Things. *Microprocessors and Microsystems*, 104708.
- Haseeb, K., Jan, Z., Alzahrani, F. A., & Jeon, G. (2022). A Secure Mobile Wireless Sensor Networks based Protocol for Smart Data Gathering with Cloud. *Computers & Electrical Engineering*, 97, 107584.
- Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. *Procedia Computer Science*, 183, 486-492.
- Iqbal, U., & Mir, A. H. (2022). Secure and practical access control mechanism for WSN with node privacy. *Journal of King Saud University-Computer and Information Sciences*, 34(6), 3630-3646.


- Jasper, J. (2021). A secure routing scheme to mitigate attack in wireless adhoc sensor network. *Computers & Security, 103*, 102197.
- John, A., & Igimoh, J. (2017). The design of wireless sensor network for real time remote monitoring of oil & gas flow rate metering infrastructure. *International Journal of Science & Research, 6*(2), 425-429.
- Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K. (2020). A survey on intrusion detection and prevention in wireless ad-hoc networks. *Journal of Systems Architecture, 105*, 101701.
- Kholidy, H. A. (2021). Autonomous mitigation of cyber risks in the Cyber-Physical Systems. *Future Generation Computer Systems, 115*, 171-187.
- Kim, A., Oh, J., Ryu, J., & Lee, K. (2020). A review of insider threat detection approaches with IoT perspective. *IEEE Access, 8*, 78847-78867.
- Kim, B.-S., Kim, K.-I., Shah, B., Chow, F., & Kim, K. H. (2019). Wireless sensor networks for big data systems. *Sensors, 19*(7), 1565.
- Kraidi, L., Shah, R., Matipa, W., & Borthwick, F. (2019). Analyzing the critical risk factors associated with oil and gas pipeline projects in Iraq. *International Journal of Critical Infrastructure Protection, 24*, 14-22.
- Kulkarni, S., Gu, Q., Myers, E., Polepeddi, L., Lipták, S., Beyah, R., & Divan, D. (2019). Enabling a decentralized smart grid using autonomous edge control devices. *IEEE Internet of Things Journal, 6*(5), 7406-7419.
- Kumar, P., Lee, S.-G., & Lee, H.-J. (2012). E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors, 12*(2), 1625-1647.
- Kumar, V., & Ray, S. (2022). Pairing-free identity-based digital signature algorithm for broadcast authentication based on modified ECC using battle royal optimization algorithm. *Wireless Personal Communications, 1*-25.
- Kuthadi, V. M., Selvaraj, R., Baskar, S., & Shakeel, P. M. (2022). Data security tolerance and portable based energy-efficient framework in sensor networks for smart grid environments. *Sustainable Energy Technologies and Assessments, 52*, 102184.
- Laaki, H., Miche, Y., & Tammi, K. (2019). Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery. *IEEE Access, 7*, 20325-20336.
- Li, X., Bao, J., Sun, J., & Wang, J. (2021). Development of circular economy in smart cities based on FPGA and wireless sensors. *Microprocessors and Microsystems, 80*, 103600.
- Lin, T., Wu, P., & Gao, F. (2022). Information security of flowmeter communication network based on multi-sensor data fusion. *Energy Reports, 8*, 12643-12652.
- Liu, J., & Labeau, F. (2021). Detection of False Data Injection Attacks in Industrial Wireless Sensor Networks Exploiting Network Numerical Sparsity. *IEEE Transactions on Signal and Information Processing over Networks, 7*, 676-688.
- Liu, L., Zhang, Z., Wu, J., & Xu, J. (2022a). Entropy optimization of degree distributions against security threats in UASNs. *Computer Networks, 205*, 108747.
- Liu, L., Zhang, Z., Wu, J., & Xu, J. (2022b). Entropy optimization of degree distributions against security threats in UASNs. *Computer Networks, 108747*.
- Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A.-R., & Tarkoma, S. (2017). Iot sentinel: Automated device-type identification for security enforcement in iot. 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS),

- Nashwan, S. (2021). AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment. *Egyptian Informatics Journal*, 22(1), 15-26.
- Ohm, M., Plate, H., Sykosch, A., & Meier, M. (2020). Backstabber's knife collection: A review of open source software supply chain attacks. *Detection of Intrusions and Malware, and Vulnerability Assessment: 17th International Conference, DIMVA 2020, Lisbon, Portugal, June 24–26, 2020, Proceedings 17*,
- Panahi, U., & Bayılmış, C. (2022). Enabling secure data transmission for wireless sensor networks based IoT applications. *Ain Shams Engineering Journal*, 101866.
- Premkumar, M., & Sundararajan, T. (2020). DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. *Microprocessors and Microsystems*, 79, 103278.
- Pruthi, V., Mittal, K., Sharma, N., & Kaushik, I. (2019). Network layers threats & its countermeasures in WSNs. *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*,
- Qiu, T., Chen, N., Li, K., Qiao, D., & Fu, Z. (2017). Heterogeneous ad hoc networks: Architectures, advances and challenges. *Ad Hoc Networks*, 55, 143-152.
- Rhim, H., Abassi, R., Tamine, K., Sauveron, D., & Guemara, S. (2020). A secure network coding-enabled approach for a confidential cluster-based routing in wireless sensor networks. *Proceedings of the 35th Annual ACM Symposium on Applied Computing*,
- Rouhani, S., Belchior, R., Cruz, R. S., & Deters, R. (2021). Distributed attribute-based access control system using permissioned blockchain. *World Wide Web*, 1-28.
- Santos-González, I., Rivero-García, A., Burmester, M., Munilla, J., & Caballero-Gil, P. (2020). Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks. *Information Systems*, 88, 101423.
- Shahid, H., Ashraf, H., Ullah, A., Band, S. S., & Elnaffar, S. (2022). Wormhole attack mitigation strategies and their impact on wireless sensor network performance: A literature survey. *International Journal of Communication Systems*, 35(16), e5311.
- Shamshiri, R. R., Hameed, I. A., Thorp, K. R., Balasundram, S. K., Shafian, S., Fatemieh, M., Sultan, M., Mahns, B., & Samiei, S. (2021). Greenhouse automation using wireless sensors and IoT instruments integrated with artificial intelligence. *Next-generation greenhouses for food security*.
- Sharma, H., Haque, A., & Blaabjerg, F. (2021). Machine learning in wireless sensor networks for smart cities: a survey. *Electronics*, 10(9), 1012.
- Sundaram, S. Subscribe to Newsletter.
- Swessi, D., & Idoudi, H. (2022). A survey on internet-of-things security: threats and emerging countermeasures. *Wireless Personal Communications*, 124(2), 1557-1592.
- Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber threats to industrial IoT: a survey on attacks and countermeasures. *IoT*, 2(1), 163-186.
- William, P., Choubey, A., Chhabra, G., Bhattacharya, R., Vengatesan, K., & Choubey, S. (2022). Assessment of hybrid cryptographic algorithm for secure sharing of textual and pictorial content. *2022 International Conference on Electronics and Renewable Systems (ICEARS)*,
- Xiong, R., Cao, J., & Yu, Q. (2018). Reinforcement learning-based real-time power management for hybrid energy storage system in the plug-in hybrid electric vehicle. *Applied Energy*, 211, 538-548.
- Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaniiche, N., Chehab, A., & Malli, M. (2020). Cyber-physical

- systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, 77, 103201.
- Yin, X., & Li, S. (2019). Trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, 2019, 1-10.
- Zaminkar, M., & Fotohi, R. (2020). SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism. *Wireless Personal Communications*, 114(2), 1287-1312.
- Zhang, C., Jia, D., Wang, L., Wang, W., Liu, F., & Yang, A. (2022). Comparative research on network intrusion detection methods based on machine learning. *Computers & Security*, 102861.
- Zhu, X. (2021). Complex event detection for commodity distribution Internet of Things model incorporating radio frequency identification and Wireless Sensor Network. *Future Generation Computer Systems*, 125, 100-111.

Author Information

Ayuba John

 <https://orcid.org/0000-0003-0496-765x>


Universiti Teknologi Malaysia

Faculty of Computing, UTM

Malaysia

Contact e-mail: john@graduate.utm.my

Ismail Fauzi Isnin


 <https://orcid.org/0000-0002-9765-3491>

Universiti Teknologi Malaysia

Faculty of Computing, UTM

Malaysia

Syed Hamid Hussain Madni

 <https://orcid.org/0000-0002-3816-1382>

Universiti Teknologi Malaysia

Faculty of Computing, UTM

Malaysia
