DOI: http://dx.doi.org/10.26483/ijarcs.v16i3.7241

Volume 16, No. 3, May-June 2025

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

AN IN-DEPTH ANALYSIS OF WSN SECURITY PROTOCOLS: A SURVEY AND PROSPECTS FOR THE FUTURE

J. Kanagaraj
Ph. D Research Scholar, Department of Computer Science,
Nehru College of Management, Affiliated with Bharathiar University,
Nehru Gardens, Thirumalayam Palayam,
Coimbatore - 641105, TamilNadu, India.

Dr. M. Sengaliappan
Associate Professor and Head, Department of MCA,
Nehru College of Management, Affiliated with Bharathiar University,
Nehru Gardens, Thirumalayam Palayam,
Coimbatore - 641105, TamilNadu, India

Abstract: Among the many possible networking systems with intriguing potential opportunities in the future, "Wireless Sensor Networks (WSNs)" has emerged as a competitor. Deployment is made easier with these compact, cheap, and sophisticated "Sensor Nodes (SNs)"; the number of SNs needed depends on the area of coverage and applications. Integrated systems for control, the medical field, ecological tracking (including the observation of volcanoes, agricultural practices, and governance), as well as the identification of sources of radioactivity, are among their prevalent uses. Security within WSN remains a major concern and a continuing area of study, despite its promising qualities. The design, adverse installation site, and unsecured routing system of deployed SNs make them susceptible to a wide range of security threats. WSNs remain vulnerable because sensor nodes have limited bandwidth, range, processing power, and storage. Despite extensive research improving applications and quality of life, fully securing these resource-constrained networks is still challenging. This paper conducted a deep survey that tailored WSN communication threats and examines the key risks and necessary security measures. Additionally, it presents a significant literature review of current security techniques for WSN settings, including "Cryptography," "Key-Management" "Secure-Routing," "Intrusion-Detection System (IDS)," and "Hashing Message-Authentication Code protocols. It concludes by outlining specific challenges in further study that will need attention to empower the security mechanism in WSN.

Keywords: Wireless Sensor Networks, Security, Cryptography, Intrusion Detection System, Key management, hashing algorithms

1. INTRODUCTION

Multiple SNs within a WSN work together to evaluate and store data; they may also communicate with various other SNs across the network. The WSN continues to be widely used because of its efficacy and affordability. A large percentage of WSN uses revolve around environmental monitoring and surveillance [1]. Integrated microprocessors and RF transmitting devices allow these components to operate as sensors. The SN possesses the ability to temporarily record observed information and undertake fundamental computations owing to its microprocessor's storage and CPU. Figure 1 shows the general design of a WSN, and the following is the basic idea of how an SN works:

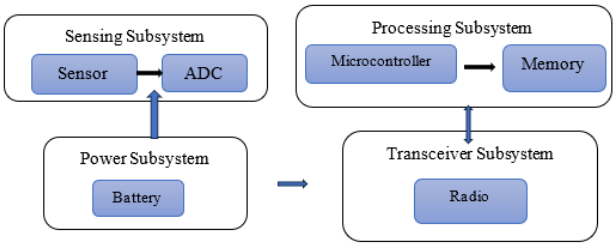

Figure 1: WSN's Standard Architecture

Multiple SNs, with every SN including 4 fundamental subsystems, combine to create a WSN. Each includes a "Sensing-Subsystem", "Processing-Subsystem", and "Transceiver-Subsystem" along with a "Power-Subsystem" [2]. Nonetheless, the SN module might consist of more subsystems according to the particular application's requirements. Unique auxiliary parts could include things like power generators, "GPS-Subsystem" and "Mobilizer-Subsystem" types of gadgets, and such. Whenever the SNs require knowledge of their position to do things like maintain their topology or route traffic, a GPS-Subsystem could be added. To facilitate the movement among their SNs, certain applications make use of the Mobilizer-Subsystem.

(i) Sensing-Subsystem: The sensor that it uses and ADC are the two main parts that make this together. The sensors collect data from their surroundings and turn it into an AC signal. The ADC subsequently digitizes the original AC signal. Transferring the signal that was detected into the Processing-Subsystem follows its digitization.

(ii) Processing-Subsystem: The sensors may then use this in conjunction with the device that stores information to do basic calculations using the information they have detected. Every sensing action is controlled by this part of the system. The 3 different states “Active-State (AS)”, “Sleep-State (SS)”, and “Idle-State (IS)” is supported by this Processing-Subsystem. Various information processing activities are constantly performed by every element within the Processing-Subsystem inside the AS. In SS, the Processing-Subsystem elements don't do anything. The Processing-Subsystem automatically restarts the function once an indicator gets activated, thus this condition preserves additional energy. Zero-sensing processing will take place while the Processing-Subsystem stands in an IS state. Nevertheless, it completes its internal processing of local information [3].

(iii) Transceiver-Subsystem: Connecting the SN to the network's resources is the primary function of this part of the

system. Following the context, either of the 2 methods of communication may be used. In some cases, the SNs can communicate with each other. Different applications promote collaboration among SNs and "Sink Node (SiN)" and make use of SiNs themselves. There are 4 possible states for the Transceiver-Subsystem: "Send-State (SeS)", "Receive-State (RS)", SS, and IS. The sensing device or SiN may receive information from the SNs once they have been configured by the SeS. Owing to the RS, the SN may receive information from various SNs. Once there is zero active connection between the SNs, the IS gets triggered. The idle mode of operation, which conserves energy, is probably the most prevalent SN operation. Lastly, once there isn't any requirement for communication between SNs, the Transceiver-Subsystem has been assigned to SS [4].

(iv) Power-Subsystem: The fundamental component of a WSN framework is this. A battery is essential for any SN. The whole detecting, analyzing, and communication procedure is set in motion by this unit. The SNs' potency, however, is very finite. Therefore, it is essential to fully use the potential of the SNs. To function, the SNs depend on all 4 of these subsystems. The system's goal can only be accomplished by the combined efforts of each of these subsystems.

Even though SNs are capable of working alone, there are instances in which they're required to communicate with different SNs. When two SNs want to exchange information with each other, they employ RF transceivers. At its core, SNs are merely portable devices that can sense their immediate surroundings, analyze them, and then send the results to other SNs. There are two primary manners by which SNs may communicate with one another: Direct-Communication and Indirect-Communication [5].

Nevertheless, the energy limits place severe limitations on these SNs. The majority of WSN deployments occur in harsh circumstances in which it is impractical to repair or replenish the batteries. So, to make the best out of SNs' energy and prolong the lifespan of WSN, it is important to use it effectively [6]. The SN would inevitably die because of inefficiency in energy utilization. A SN is capable of carrying out its task using only an appropriate amount of energy. The RF component of SNs, for instance, uses greater power. Energy consumption and the lifespan of a system are, hence, closely related. Indirectly, the lifespan of SNs is related to their usage of energy. A longer lifespan for the network is associated with lower energy use.

When it comes to WSNs, authenticating messages is a powerful tool for stopping the transmission of compromised or illegal communications. That's why a plethora of Cryptosystems-based authentication methods for message techniques have emerged. Nevertheless, plenty of those encounter a shortage of scaling, vulnerability to SN-compromising threats, as well as high transmission and processing costs. Current methods are not optimal concerning computing cost, consumption of energy, "Packet-Delivery Ratio (PDR)", Delay, or storage utilization. Additional improvements are needed.

Problem Statement: Sophisticated Modulating, Network Coding, along with techniques for encryption have been frequently employed to guarantee data privacy; nevertheless, these methods often raise the rate of transmission and, thus, demand greater amounts of energy. Unfortunately, the energy overhead caused by secure communications isn't addressed under the majority of WSN protocols that are presently in existence. There are a plethora of authentication systems that fall into two broad classes: "Public-Key (PuK)" and "Symmetric-Key (SmK)". For instance, this method is ineffective in multicast networking due to the SmK's inadequate scalability. Once the total volume of messages transferred exceeds a certain limit using the confidential polynomial-based authentication of messages mechanism, the network becomes entirely disrupted and its polynomial basis might be entirely accessed. While PuK has a lot of computing expenses, novel research on "Elliptic Curve Cryptography (ECC)" reveals that PuK methods may be better in storage use, privacy resiliency, and computational challenge due to their effortless administration of keys. Insufficient effectiveness and inadequate scaling (the cutoff issue) are two of ECC's drawbacks. Therefore, it is necessary to provide an architecture that can resemble WSN-specific encryption protocols, enabling researchers to strike a compromise between performance and safety while doing a thorough multi-level protocol analysis.

Paper Contribution: The research contributions to this survey work have been outlined below:

- The article begins by outlining the many problems and difficulties that WSNs face. Next, it lays out the specifics of the threat framework that could be used to ensure the safety of communications through WSNs.
- Additionally, it delves into the need for security measures and the many types of attacks that might occur when communicating scenarios with WSNs.
- This paper also includes a taxonomy of the several WSN security protocols.
- In the end, it draws attention to a few problems with the current state of research that will need fixing soon.

Paper Organization: Recent survey articles from reputed journals regarding WSN security protocols are discussed in Section 2, Section 3 covers every aspect of the threat framework that is specific to the security of WSN-oriented communication, as well as the security objectives, potential attacks, and a classification of WSN protocols for security, Section 4 provides an discussion of the current protocols of WSN with its shortcomings and suggests the optimal requirements for new protocols, and Section 5 concludes the article with future dimensions.

2. RELATED WORKS

The researchers of [7] present a review of the research focusing on issues related to "Energy-Efficiency (EE)", attacker identification, and network connection in WSN. To maximize the efficiency of the SNs' energy usage, several methods have been studied. Methods like "Artificial-Immune Systems" and "Wavelet-Analysis" were chosen to deal with both the coverage and connection issues of WSN. The review of literature covers current research on WSN and describes the problems with and potential solutions to EE, attacker identification, and network connectivity. At the end of the survey, they pointed out where current research is lacking and provided some suggestions for where it can go from here in terms of improving WSN performance.

In [8], the researchers highlight the major, incompatible problems that WSNs have with security and

energy. The more complicated the security measures, the more power they will use. Conventional security solutions such as KM and encryption have shown to be ineffective in WSNs because of their restricted energy and changeable topology. This review paper uses ML techniques to assess the security, routing, and clustered challenges that WSNs encounter with their associated difficulties. Thus, in support of WSNs with their many challenges, this review article provides a high-level summary of ML methods.

Numerous ML methods that are used to identify outliers in WSN data have been investigated by the researchers [9]. In the context of problems like EE along with data credibility, this literature review stresses the need for precise anomaly detection without compromising data quality. This paper's overarching objective is to present a review of security techniques having an emphasis on both online and offline identification modes, increasing performance whilst decreasing resource consumption. This study highlights the importance of identifying anomalies in WSNs, it delves into ML approaches and demonstrates their efficacy in improving the security of data in IoT applications and accurately detecting anomalies.

By highlighting the major issues and limitations of the present methodology, the researchers in [10] present a comprehensive evaluation of both security and energy strategies in WSNs. In enormous scale or scarce resources environments, traditional approaches often encounter issues including increasing latency, difficulties obtaining real-time optimum solutions, and unnecessary computational overhead. This research delves into the current approaches and highlights the potential of Deep-Learning.

The survey carried out by the researchers of [11] aims to examine current security methods that have been developed to reduce the impact of such attacks on IoT networks. They focused on Trust & Probe type methods when conducting a systematic study of compact security techniques. Defending IoT networks without sacrificing efficiency is possible with the help of these technologies. In addition, the research investigation compares and contrasts different approaches, assessing them according to security measures, the kinds of attacks they counter, and important performance indicators like power use and reaction times. This research offers useful insights into the efficiency of different security measures in defending networks facilitated by the WSNs from contracting cyber-attacks through its comparison method.

3. METHODOLOGIES

WSNs comprising a significant amount of distributed SNs are made up of self-configuring, battery-operated SNs that collect information in response to user-defined commands. Regardless of WSNs' numerous applications in industry and commerce, among them in the areas of medical services, the armed forces, and household security, several architectural and operating constraints influence the general functioning of the network. Because of those variables, investigations are ongoing and no perfect solutions have been discovered currently [12].

Despite several issues, experts have focused on “Military-WSN (MWSN)” shortcomings in security, which are certainly being evaluated as a possible concern that needs fixing. After taking a deeper look at various issues related to WSN activities, it becomes clear that a combination of circumstances, including a restricted-energy supply and a shortage of computing resources, is the primary cause of every single functional restriction in WSNs. Thus, it's very evident that WSNs can't deliver affordable energy management and react adequately to advanced connectivity requirements considering so minimal availability of resources.

Security is emerging as a major concern within the realm of MWSNs. Fortunately, there are currently several promising encryption protective methods that could help address this problem. These methods are currently making considerable strides and are undoubtedly applied to different types of networking infrastructures, such as ad-hoc ones. Most SNs, involving MWSNs, communicate by broadcasting their messages through a radio channel; this makes them vulnerable to intrusion and other forms of fraudulent behavior. When trying to conduct unlawful practices for hostile penetration in MWSN, an intruder SN may continuously monitor the originating SN's actions.

According to this standardized threat situation with MWSNs, a malicious SN keeps track of what an authorized SN is capable of at all times. Additionally, it emphasizes that a malicious SN that continually pays attention to the channel for communication may simply trace the route of transmission for the communication directly to its originating SN while the system is overwhelmed with messages. The data packet's strength of signal, being much greater inside that source's communicating spectrum, has been determined to initiate the attack. Furthermore, the above-attacking hypothesis provides the opportunity for concentrating the research's focus on the fundamentals of MWSN-originating location secrecy.

3.1 MWSN: Attacks Classification

Security threats to MWSNs may take many forms, including intrusions into private information, monitoring of network traffic, and even physical assaults that disrupt 802.11 MAC-Layer WSN transmission to compromise data integrity or alter it without authorization. Intending to impact the overall communication efficiency of several crucial and basic network functions, attacks typically additionally employ a packet-dropping technique [13]. The following are examples of major invasions and attacks that occurred when MWSN networks were operational:

(i) Active-Attacks: Most often, an active assault happens whenever an attacker gains unapproved possession of long-term observed information and then modifies it inside a transmission channel. The privacy needs of MWSN have been investigated and comprehended concerning those attack kinds.

(ii) Passive-Attacks: Passive attacks happen when a malicious element constantly monitors and senses the transmission channel, violating the right to privacy along with the integrity of information.

(iii) Attacks Impacted by Network Availability: This primarily pertains to DoS attacks which may potentially occur across any tier of MWSNs.

(iv) Disruption of the Trust in the Service: An outside entity pushes the operating element of an MWSN by accepting compromising and destructive information in an attempt to penetrate the entirety of the network through an SN or SiN; this has become recognized as another type of attack.

(v) Attacks Related to the Authentication Procedure: An attacker may get access to the transmission channel and use it to change sensitive information with this kind of attack.

As a result of categorizing various types of assaults on networking surfaces, the requirements for security over enormous-scale MWSNs have been justified. Despite the widespread use of WSNs, only a fraction of the data they process is highly secret or confidential. Regarding this matter, an issue about safeguarding sensitive data emerges in MWSN, wherein multiple options have not yet been acknowledged [14]. As a result, MWSNs have different security needs than more traditional types of networks.

3.2 MWSN: Standard Security Approaches

Numerous investigators have presented numerous strategies to prevent network assaults, and these approaches are considered for particular parts of WSN networks. An attack-resistance method for WSNs is presented throughout this section.

(i) Cryptography Approaches:

The process of encryption, authorization, and an extensive number of other security procedures are all part of cryptography, a crucial tool for protecting WSNs [16]. The two main categories of cryptography are SKE and "Asymmetric-Key Encryption (AKE)". When 2 SNs exchange information, they exchange an individual SeK in SKE. Securely establishing the key becomes the difficult part of this method, which also does decryption. "PuK Cryptography" is another name for AKE; it uses two different keys, "PuK" and "Private-Key (PrK)," that are not identical. Information is protected during transmission by encrypting it using the target's SN's PuK, while the originator's SN's PrK is used for authentication. Intending to provide top-notch security measures in WSNs, this is essential to choose the appropriate cryptographic method for SNs, which are often constrained. Therefore, it can be highly advantageous when employing more effective substitutes for SKE.

The selection of encryption systems needs to be based on the factors that follow:

- To calculate energy consumption using both decryption and encryption processes.
- The amount of storage that may be used for both decryption and encryption is proportional to the length of the code.
- Both decryption and encryption execution of codes require a certain amount of RAM.
- Both the procedures for decryption and encryption add delay to the overall execution duration.
- By calculating how many SeKs both decryption and encryption functions need to operate, one can estimate how much RAM will be needed.

(ii) KM Approaches:

When connecting the SN with the rest of the system, the secret cryptography key is crucial for ensuring transmission security [17]. KM represents a cornerstone of reliable and robust security basic features. Using SeK provides a foundation that becomes essential to the cryptography security framework. Collaborating SNs employ KM techniques to build up and disseminate various keys for cryptography, including "Individual-Keys," "Even-Keys," and "Group-Keys," making them necessary for sharing data inside the network.

The whole network of communications has to be compromised once an intruder manages to locate the SeK and potentially obtains the key. As a way to prevent an intruder from gaining accessibility to those operations that are essential to the whole transmitting and communicating function. Consequently, a dependable and effective WSN architecture cannot be achieved without an appropriate KM.

Following are a few tried-and-true methods for generating a unique key for every SN:

- It is recommended that keys are loaded onto every single SN before the implementation of WSNs.
- Both the SN along the BS know the key that has been allocated to every SN.
- "Pair-Wise SeKs" towards an arbitrary set of SNs would constitute the basis for this Key-Agreement technique.
- Establish a protocol that allows the SeK to demonstrate its dependability, which implies it constitutes a SeK and is capable of carrying out its role effectively.
- An extra solid KM approach may be created by using a "Master-Key (MaK)" approach. Once the key has been generated connecting the two separate SNs, a MaK may temporarily take the role of the SeK. With these safeguards in place, attackers will have a harder time gaining access to sensitive data.
- The hacked SN along with every subsequent SN needs to reset as well as no longer employ the shared encryption key data. This procedure should be considered compulsory since there is a possibility that an intruder has captured past traffic information and could employ it to negatively impact other working SNs.
- When it comes to the drain on networking energy, key-revoking is conceived as being costly. As a result, a distributed key revoking mechanism works well.

(iii) Secure Routing:

Trustworthy data transmission services provided by WSN systems are not possible without the Secure-Routing technology [18]. When trying to send information, WSNs employ a route with multiple hops method using the RF communication channel. This makes them easy targets for hackers. Because of features like key-oriented multiple-path communication, BS decentralized administration, reciprocity approval, verification of identity, and topological architecture limitation, protocols for routing can withstand any type of attack that may affect the entire network's performance. To provide security standards for protecting information in WSNs, several successful routing mechanisms are currently devised keeping security strives in consideration. The following constitute the 3 primary approaches whereby SKE is used to classify routing techniques: "Flat-Structure Routing" has emerged as an approach to routing that ensures that every SN performs the same function; "Hierarchical-Structure Routing" has emerged as a routing approach to which distinctive SNs have received distinct functions; and "Location-Routing" has emerged as a routing method in which information concerning data within the network's environment is routed.

(iv) IDS

Investigating and removing potentially dangerous assaults sooner rather than later may significantly reduce their

effect. The IDS initially appeared in 1980 and has since proven to be a great resource for automatically identifying and notifying the system concerning network attackers. The following section provides a high-level summary of IDS, outlining their structure and discussing the various approaches used for network protection. An IDS is a network-wide set of computing tools, techniques, and resources used to detect and block malicious SN activities throughout a WSN [19]. The main goal of IDS is to identify when SNs' behaviour changes and then trigger an alert to notify the appropriate authorities of an invasion.

Two primary categories of IDS have been described as follows:

(a) Host-IDS (HIDS): The primary goal concerning HIDS is to prevent unauthorized changes to data and privacy regulations by keeping track of an individual host system. The purpose of this module is to keep surveillance towards the Host-Server, which it finds through the Host-Terminal. When gathering knowledge regarding the activities, HIDS uses a couple of sources: information gathered from log files along with both outgoing and incoming packets. One major issue concerning HIDS is the extra overhead that it generates, and this in turn negatively impacts downward the host.

(b) Network-IDS (NIDS): NIDS has been developed to keep checks on all of a network's traffic to find security holes and strike them. The whole networking infrastructure safeguarding from attackers or intruders is the primary goal of NIDS within this framework.

Problems with IDS Design:

Several features of the WSN, including its distributed environment, constraints on resources, and topology of networks, provide design issues for the IDS. Establishing secure IDS over WSNs requires meeting the subsequent challenging architectural restrictions. Modifying the Topology of Dynamic Systems, Infrastructure shortage, Lowering the Capacity to Consume Resources, Routing Protocol Variant Functionality and Simple and Convenient Physical Access

(v) HMAC

Within WSNs, HMAC offers comprehensive safety and distinct messaging authenticity by combining an encryption key in conjunction with “Hash-Function (HF)”, which significantly lessens the demand for computing on SNs [20]. An HF is a function that operates with mathematical calculations that take a numerical data result and use repeated steps to transform it towards a fixed-length result. When trying to produce a Hash-Code, the HF combines two consecutive blocks that have a predetermined dimension; the exact dimensions of these blocks remain system-specific. The Hash Method is made up of iterations through the “Hash-Value (HV)” function, whereby every iteration accepts the sequences of input regarding the most current messaging blocks and uses them to conduct subsequent iterations. The whole message gets hashed by repeating the procedure for multiple rounds when needed.

There are a few HFs that are listed below:

(a) MD: Rivest came up with this concept around 1991. The model was an extensively utilized HF that had a lot of popularity in the last several decades. Its ability to guarantee communication integrity has contributed to it being widely employed throughout the IT industry. The raw information handled by MD-5 has been organized across "Sub-Blocks (16)" with a dimension of 32-bits each of them after being split into "Block-Size (512-bits)" during processing. An error involving MD-5 had been documented in 2004. The use of an ensemble of machines allowed an attack to turn out devastating in a very short amount of time. Hence, it was recommended that MD-5 be terminated.

(b) SHA-1: A consortium known as NIST created it in 1995. It started as an alternative spanning the first SHA. There were certain issues, and the solution wasn't enough to deliver reliable security solutions. A set of approximately 160-bit outputs are generated by it. Depending upon the MD-5, which employs 512-bit blocks for analyzing inputs along with 80 cycles to compute the resulting HV, SHA-I is designed to be secure. Numerous protocols, including SSLS, made substantial utilization of it.

(c) SHA-2: Around 2004, the NIST developed this. Various versions of comparable HFs, namely "SHA-224, 256, 384, 512," are included together with it. Despite the lack of evidence of an attack that succeeded on SHA-2, the algorithm continues to be widely utilized and provides enough protection.

(d) SHA-3: Recent, more sophisticated hashing concept, SHA-3, were released by the NIST during 2012. Depending upon the "Keccak" method, SHA-3 was designed. Superior efficiency, low cost, and powerful resistive properties towards diverse attacks are merely a few of the outstanding advantages offered by this HF. Figure 2 depicts the efficiency of various security mechanism in WSN.

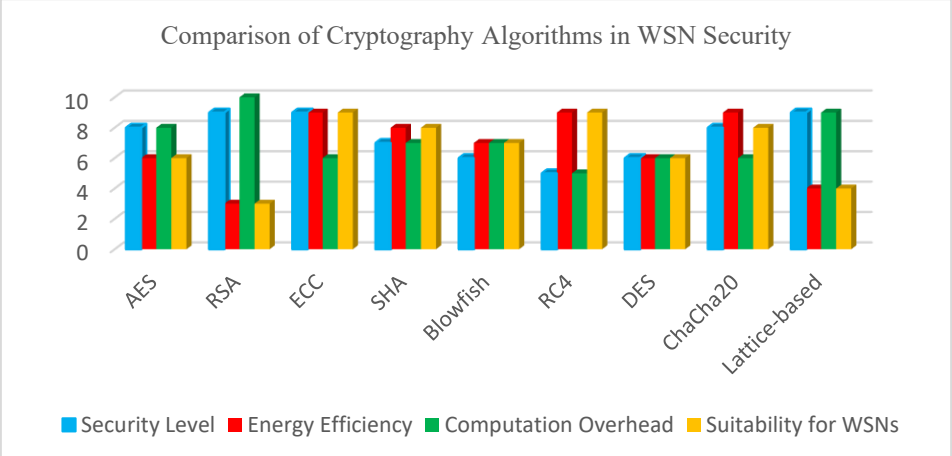

Figure 2: Comparison of cryptography Algorithms in WSN security

4. DISCUSSION OF THE STUDY

Wireless Sensor Networks (WSNs) have evolved significantly in recent years, offering vast potential across various domains. However, they remain highly vulnerable to privacy threats and intrusions. The timely detection of attackers is essential to mitigate damage, making Secure Energy-Efficient (EE) Protocols an emerging focus in WSN security. These protocols aim to identify both malicious and unintentional anomalies by monitoring system behaviour. Intrusions in WSNs typically occur in two stages: either through external attacks that compromise sensor nodes (SNs) or internal misuse where attackers exploit compromised SNs to access or manipulate sensitive data. A critical challenge arises when compromised nodes do not exhibit obvious behavioural anomalies, making detection difficult. Traditional cryptographic methods alone may not suffice, as attackers with access to targeted SNs can bypass these protections. To address this, genuine SNs must take a proactive role in monitoring peer behaviour. However, attackers may suppress abnormal behaviour in infected SNs, limiting the effectiveness of behaviour-based detection. These unresolved issues highlight the ongoing need for research in developing robust, adaptive, and energy-efficient security mechanisms tailored for Mobile WSNs (MWSNs). Comparison of WSN security techniques is shown in figure 3.

Figure 3 Comparison based on Security Strength, Energy Efficiency, and Computation Overhead for various WSN security techniques.

By breaking down current systems into their parts and looking for vulnerabilities, the suggested study hopes to solve a few interconnected research security issues with MWSNs as follows:

- **Delayed Detection of Intrusions:** Intrusions are often not detected immediately, especially when compromised nodes behave normally, leading to prolonged exposure and potential data breaches.
- **Limited Effectiveness of Traditional Cryptographic Protocols:** Standard cryptographic methods are not directly applicable in WSNs due to resource constraints and the possibility of node compromise, which may give attackers access to keys or protected data.
- **Malicious Node Behavior Concealment:** Infected sensor nodes (SNs) may not exhibit visible signs of abnormal behavior, making it difficult for the network to detect intrusions based solely on behavioral monitoring.
- **Risk of Internal Attacks:** Once a node is compromised, attackers can gain access to sensitive data and perform unauthorized actions within the network, mimicking legitimate communication.
- **Lack of Immediate Peer Detection:** Genuine SNs are expected to monitor peer activities to detect anomalies, but this is challenged when malicious SNs mask their activities or manipulate monitoring mechanisms.
- **Inadequate Intrusion Response Mechanisms:** The existing protocols struggle to differentiate between genuine and fraudulent nodes early in the attack lifecycle, leading to increased vulnerability.
- **Dynamic and Unpredictable Network Topology:** Mobility in MWSNs complicates consistent monitoring and coordination for intrusion detection, making real-time security enforcement more difficult.

The challenge in this research is to develop a computationally efficient architecture for Mobile Wireless Sensor Networks (MWSNs) that can provide a robust level of security, while simultaneously ensuring energy efficiency and maintaining networking performance. Achieving this balance is crucial, as it remains a significant issue in the development of MWSNs.

5. CONCLUSION

This review paper has thoroughly explored the security needs and potential threats in Wireless Sensor Network (WSN)-based communication systems. It has also provided an overview of the latest interoperability efforts in WSNs and detailed several WSN configurations. A classification of current security protocols for WSN communication has been presented, highlighting the existing protocols and survey results related to energy efficiency (EE) and secure routing. One critical aspect covered is the design of encrypted EE

protocols for routing, which need to strike a balance between limited energy consumption, avoiding excessive resource use, and minimizing overall energy degradation during data transmission. The paper suggests that ensuring privacy in routing requires developing protocols that are energy-efficient without compromising security. This review serves as a valuable resource for selecting suitable protocols and approaches to enhance the security and efficiency of WSNs. The paper concludes by outlining future research challenges, particularly in the development of security protocols that incorporate energy efficiency in mobile WSN-based communication systems, which remains an area requiring further exploration.

REFERENCES

[1]. J. P. Rojas et al., "Self-Powered End-to-End Wireless Sensor Network for Geophysical Explorations," in IEEE Systems Journal, vol. 19, no. 1, pp. 107-118, March 2025, doi: 10.1109/JSYST.2025.3532698.

[2]. G. H. Adday, S. K. Subramaniam, Z. A. Zukarnain and N. Samian, "Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey," in IEEE Access, vol. 12, pp. 22938-22977, 2024, doi: 10.1109/ACCESS.2024.3362889.

[3]. O. A. Amodu et al., "Deep Reinforcement Learning for AoI Minimization in UAV-Aided Data Collection for WSN and IoT Applications: A Survey," in IEEE Access, vol. 12, pp. 108000-108040, 2024, doi: 10.1109/ACCESS.2024.3425497.

[4]. R. Ahmad, W. Alhasan, R. Wazirali and N. Aleisa, "Optimization Algorithms for Wireless Sensor Networks Node Localization: An Overview," in IEEE Access, vol. 12, pp. 50459-50488, 2024, doi: 10.1109/ACCESS.2024.3385487.

[5]. İ. H. Turan, D. Yildiz, S. Demirci and M. Sayit, "Analyzing the Impact of Transmission Strategies on Localization Performance in Wireless Sensor Networks," in IEEE Access, vol. 13, pp. 37673-37689, 2025, doi: 10.1109/ACCESS.2025.3545263.

[6]. M. -R. Mortada, A. Nasser, A. Ramadan, K. -C. Yao and A. Mansour, "Location Information-Based Routing Protocol for Energy Harvesting Cognitive Radio Wireless Sensor Network," in IEEE Access, vol. 13, pp. 9965-9980, 2025, doi: 10.1109/ACCESS.2024.3517741.

[7]. A. K. Rai, M. Singh, V. Dwivedi, A. K. Pandey, and A. Kapoor, "A Review on QoS based Protocols in Wireless Sensor Network," 2024 International Conference on IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2024, pp. 1518-1523, doi: 10.1109/ICICAT62666.2024.10923496.

[8]. P. Srujana, J. Priyanka, K. Gurucharan and M. Rajanbabu, "Exploring ML Solutions for Challenges in WSN Development: A Comprehensive Survey," 2024 IEEE Wireless Antenna and Microwave Symposium (WAMS), Visakhapatnam, India, 2024, pp. 1-4, doi: 10.1109/WAMS59642.2024.

[9]. B. Baykal, B. Saoud, I. Shayea and R. Leila, "Outlier Detection in Wireless Sensor Networks Based on Machine Learning: Review," 2024 IEEE 16th International Conference on Computational Intelligence and Communication Networks (CICN), Indore, India, 2024, pp. 432-437, doi: 10.1109/CICN63059.2024.10847563.

[10]. S. Shafiuddin and K. H. Krishna, "Enhancing Energy Efficiency and Security in Wireless Sensor Networks: A Survey and Proposed Methodology Integrating Prediction Algorithms and Deep Neural Networks," 2024 IEEE 6th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), Hamburg, Germany, 2024, pp. 441-446, doi: 10.1109/ICCCMLA63077.2024.10871374.

[11]. M. Deore and C. Gosavi, "Detection and Prevention Various Network Attacks Using Soft Computing Approaches: An Overview," 2025 1st International Conference on AIML-Applications for Engineering & Technology (ICAET), Pune, India, 2025, pp. 1-6, doi: 10.1109/ICAET63349.2025.10932241.

[12]. K. Avila, P. Sanmartin, D. Jabba, and J. Gomez, ‘‘An analytical survey of attack scenario parameters on the techniques of attack mitigation in WSN,’’ Wireless Pers. Commun., vol. 122, no. 4, pp. 3687–3718, Feb. 2022, doi: 10.1007/s11277-021-09107-6.

[13]. J. Karoliny, B. Etzlinger, R. Khanzadeh, A. Springer and H. -P. Bernhard, "Network Support Layers Trustworthiness Computation for Wireless Networks," in IEEE Transactions on Communications, vol. 73, no. 3, pp. 1879-1894, March 2025, doi: 10.1109/TCOMM.2024.3453388.

[14]. S. Padmanabhan, R. Maruthi, and R. Anitha, ‘‘An experimental study to recognize and mitigate the malevolent attack in wireless sensors networks,’’ Global Transitions Proc., vol. 3, no. 1, pp. 55–59, Jun. 2022, doi: 10.1016/j.gltp.2022.04.013.

[15]. H. Hakami, M. Faheem and M. Bashir Ahmad, "Machine Learning Techniques for Enhanced Intrusion Detection in IoT Security," in IEEE Access, vol. 13, pp. 31140-31158, 2025, doi: 10.1109/ACCESS.2025.3542227.

[16]. A. Bilal, S. M. N. Hasany, and A. H. Pitafi, ‘‘Effective modelling of sinkhole detection algorithm for edge-based Internet of Things (IoT) sensing devices,’’ IET Commun., vol. 16, no. 8, pp. 845–855, May 2022, doi: 10.1049/cmu2.12385.

[17]. H. Zhou, H. Zou, P. Zhou, Y. Shen, D. Li and W. Li, "CBCTL-IDS: A Transfer Learning-Based Intrusion Detection System Optimized With the Black Kite Algorithm for IoT-Enabled Smart Agriculture," in IEEE Access, vol. 13, pp. 46601-46615, 2025, doi: 10.1109/ACCESS.2025.3550800.

[18]. D. Gutierrez-Rojas et al., "Detection and Classification of Anomalies in WSN-Enabled Cyber-Physical Systems," in IEEE Sensors Journal, vol. 25, no. 4, pp. 7193-7204, 15 Feb.15, 2025, doi: 10.1109/JSEN.2024.3520507.

[19]. S. Afnan Birahim et al., "Intrusion Detection for Wireless Sensor Network Using Particle Swarm Optimization Based Explainable Ensemble Machine Learning Approach," in IEEE Access, vol. 13, pp. 13711-13730, 2025, doi: 10.1109/ACCESS.2025.3528341.

[20]. R. K. Dhanaraj, L. Krishnasamy, O. Geman, and D. R. Izdrui, ‘‘Black hole and sink hole attack detection in wireless body area networks,’’ Comput., Mater. Continua, vol. 68, no. 2, pp. 1949–1965, 2021, doi: 10.32604/cmc.2021.015363.