Partners Universal International Innovation Journal (PUIIJ)
Volume: 03 Issue: 03 | May-June 2025 | ISSN: 2583-9675 | www.puiij.com

Enhancing WSN Reliability: A Survey of Security, Privacy, And Routing Strategies

N.Karthick[1], Dr. K.Ranjithsingh[2]

[1]Ph.D. Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.
[2]Assistant Professor and Research Supervisor, Department of Information Technology, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.

Abstract - Wireless sensor networks (WSNs) have attracted significant attention due to their diverse applications in areas like environmental monitoring, precision agriculture, and industrial automation. However, their reliance on resource-constrained sensor nodes with open wireless communication channels presents distinct security and privacy challenges. This research paper delves into these challenges comprehensively and examines existing solutions. It investigates the ramifications of security attacks such as stealth node compromise on the integrity and dependability of WSNs. Additionally, it explores crucial security mechanisms including encryption, authentication, and access control, alongside privacy-preserving techniques aimed at anonymizing data and ensuring unique privacy measures. Furthermore, the paper discusses the intricate relationship between security, privacy, and routing efficiency, while shedding light on unresolved research queries and future avenues for safeguarding WSNs. This study serves as a beneficial reference for both investigators and professionals seeking to grasp and address issues concerning WSN security and routing.

Keywords: WSN, Privacy Techniques, Security Techniques, Routing Types, Routing Strategy, and Routing Techniques.

1. INTRODUCTION

Wireless sensor networks are a fascinating emerging technology that might transform the way data is collected in many different fields. It consists of multiple sensor nodes that are geographically dispersed and work together to monitor physical or environmental conditions like temperature, sound, vibration, pressure, motion, or even pollutants (Kizza, J.M., 2024) [1]. One key benefit of WSNs is their distributed nature. Unlike traditional centralized networks with a single point of control, sensor nodes of WSNs are scattered throughout a designated area. This distributed deployment makes them ideal for monitoring large or remote environments that would be difficult or expensive to cover with traditional methods. However, a key characteristic of WSNs is their operation under resource constraints. These WSNs have limited processing power, memory and battery life typically formed of small, affordable sensor nodes. It makes them a cost-effective solution for various applications. Furthermore, WSNs offer a flexible and adaptable solution for monitoring tasks. The number of sensor nodes can be flexibly adjusted to match the specific requirements of the application. This scalability combined with real-time data collection from the sensor nodes, allows for immediate analysis and response to changing conditions.

WSNs have gathered significant interest due to their diverse applications. They can be deployed for environmental monitoring, precision agriculture, industrial process control, healthcare, and even smart city

infrastructure management. In environmental monitoring, WSNs are used to track air and water quality, monitor soil conditions, and detect forest fires in realtime, enabling proactive measures to protect the surroundings. Precision agriculture uses sensor networks to optimize irrigation systems, track crop health for targeted interventions, and improve overall agricultural efficiency. WSNs are used in the healthcare industry for patient monitoring, remote health diagnostics, and medication management which improves patient care and convenience (Adil, M., et. al., 2022) [2]. WSNs also contribute significantly to infrastructure security by monitoring critical infrastructure for breaches, structural integrity, and environmental changes. It plays a major role in smart city programs by optimizing traffic flow, building energy efficiency, and air quality management contributing to a more efficient and sustainable urban environment (Faris, M., et. al., 2023) [3]. Finally, WSNs have enormous potential for early warning systems for disasters. Sensor networks can detect earthquakes, floods, and other potential disasters, providing crucial warnings that can save lives and property (Kandris, D., et. al., 2020) [4]. As WSNs become increasingly integrated into these critical areas, they collect vast amount of data. This in turn fuels the growth of WSN in a vast array of applications.

Despite their potential in vast fields, WSNs face security and privacy hurdles. Scattered, resource-limited sensor nodes are vulnerable to physical tampering, potentially exposing sensitive. Open lines of communication make security even more vulnerable by allowing eavesdropping on critical information. WSNs are also vulnerable to attacks at the network level like wormhole attacks creating false information tunnels, while Sybil attacks disrupt routing or launch denial-of-service attacks (Alansari, Z., et. al., 2022) [5]. Additionally, selective forwarding or sinkhole attacks can disrupt communication and compromise Quality of Service (QoS). Furthermore, the data itself raises privacy concerns. Without encryption, unauthorized access can reveal details about the environment or individuals. Location data from sensor nodes can also be used to infer information or track individuals. To address these challenges, strong security measures are required. Encryption, access control, and location anonymization techniques like k-anonymity are crucial for securing data and ensuring reliable WSN operation. By overcoming these challenges, WSNs can remain a powerful tool for data collection across various fields.

2. LITERATURE SURVEY

Faris, M., et. al., 2023 [3] analyzed different attack types across various WSN layers, categorized threats, and explored potential solutions using existing algorithms. Furthermore, the paper acknowledged limitations in current solutions and proposed a framework for building an IDS specific to WSNs emphasizing areas where further research is needed. Rehman, A., et. al., 2022 [6] proposed blockchain technology, a secure and distributed ledger system to address security vulnerabilities in WSNs for IoT. This explores how blockchain can be integrated with existing clustering techniques to optimize data flow and network efficiency. Hasan, M.Z., et. al., 2023 [7] examined network security in WSNs and IoT systems highlighting the prevalence of human-caused cyber threats and explored Message Rapid Spanning Tree Protocol (RSTP) as a more efficient option than Bridge Data Unit Protocol (BPDU). Ebrahimi, Y., et. al., 2022 [8] proposed a two-fold approach, an energy-saving scheme for overloaded nodes near the base station (BS) and a Cross-Layer Transmission Range Adjustment technique that adjusts transmission ranges to confuse attackers extending network life and enhanced the anonymity of the base station, making it a more secure communication hub. Uthumansa, A., et. al., 2020 [9] investigated how malicious attacks disrupt routing in mobile ad-hoc networks (MANETs) by analyzing Blackhole, Grayhole, and Wormhole attacks. Evaluation is done through Average Data Dropping Rate (ADDR), Average End-to-End Delay (AEED), Packet Delivery Ratio

(PDR), throughput, and Simulation Processing Time at Intermediate Nodes (SPTIN). These attacks significantly reduced successful data delivery and increased data drops compared to Wormhole attacks.

Qi, X., et. al., 2020 [10] proposed an asymmetric key encryption scheme based on an elliptic curve for securing WSN data focusing on reducing energy consumption through optimized key management, leveraging privacy homomorphism to achieve end-to-end data encryption and ensuring confidentiality. To guarantee data integrity during transmission, the method also incorporates a hop-by-hop verification method. Jiang, H., et. al., 2020 [11] discussed the core concepts of differential privacy and its variations and how this technique can be applied to social network analysis. These tasks included degree distribution analysis, subgraph counting, and edge weight analysis. Differential privacy also protects individual data privacy while sharing statistical information. Chen, Y., et. al., 2022 [12] proposed Protection Scheme Based on Sector Phantom Routing (PSSPR) aimed at safeguarding the privacy of source locations in WSN. PSSPR used phantom nodes to confuse attackers which was created strategically to hide the real source of data while still allowing data to reach the destination with minimal extra communication overhead. Simulations showed that PSSPR offered strong protection for source location while b eing efficient. Lilhore, U.K., et. al., 2022 [13] proposed a depth-controlled, energy-balanced routing protocol for underwater sensor networks by adjusting the depth and swapping low-energy nodes for high-energy ones, balancing energy usage and improving network performance. This approach utilized advanced algorithms, achieving better data transmission and lower energy consumption in simulations. Patidar, Y., et. al., 2024 [14] analyzed existing routing protocols in WSNs and IoTs, choosing the right routing method for efficient and reliable data transmission. It discussed various routing methods including flat, hierarchical, location-based, and energy-aware routing, and divided the discussion into proactive, reactive, and advanced clustering-cum-routing methods. It also addressed optimizing network performance for cluster count, throughput, and lifetime and provided a comparative analysis of different protocols.

Roberts, M.K., et. al., 2023 [15] proposed an improved high-performance cluster-based secure routing protocol for WSNs in the IoTs. It improved data management through features like energy efficiency, reduced data size, and attack detection. Its effectiveness was evaluated using various metrics, including its ability to detect attacks, conserve energy, and extend network lifetime. Dogra, R., et. al., 2023 [16] proposed an Improved Region-Based Routing Protocol REERP for WSNs in the IoT designed to extend network lifetime. The approach relied on techniques including the selection of cluster heads based on residual energy, multi-hop communication across the network, and an energy hole reduction method. This protocol achieved superior performance compared to existing protocols in terms of lifetime, energy consumption, and data delivery. Priyadarshi, R., et. al.,2019 [17] introduced an enhanced Geographical Energy-Aware Routing (GEAR) protocol for WSNs, where node separation was based on Global Positioning System (GPS) determined positions. Nodes near the central gateway or faraway base station are transmitted directly. Distant nodes were grouped by location and selected a leader based on energy levels. This protocol improved network lifetime, energy consumption, and packet transmission compared to existing protocols. Olivia, D., et. al., 2021 [18] proposed a dynamic routing protocol for Mass Casualty Incident (MCI) prioritized critical patients while considering data reliability, delay, network capacity, and battery life. It also distributed data load, managed buffer space based on urgency, and utilized a streamlined routing method. Kandris, D., et. al., 2023 [19] proposed a comprehensive overview of hierarchical routing protocols, a key approach for extending the lifetime of WSNs in 5G and IoT deployments. It explored LEACH, the first protocol of this type, and analyzed 18 similar protocols. By comparing them and simulating LEACH against three of its descendants, LEACH was the most energy saving protocol to extend the lifespan of sensor networks.

This research aims to comprehensively examine the security and privacy challenges faced by Wireless Sensor Networks and analyze existing solutions. The paper will investigate the impact of security attacks on WSNs and explore various security mechanisms such as encryption, authentication, and access control. It will further delve into privacy-preserving techniques and analyze the interplay between security, privacy, and routing efficiency within WSNs. Finally, the paper will identify unresolved research questions and discuss future directions for securing and safeguarding WSNs. This paper delves into the world of WSNs by exploring their applications, security challenges, and efficient routing protocols. The introduction section briefly introduces WSNs and their diverse applications. In literature review section, summarizes the existing research on WSN security challenges and routing protocols. The WSN security section discusses security threats faced by WSNs at different network layers and explores existing security solutions. The privacy-preserving technique section explains the importance of privacy in WSNs and relevant approaches to safeguard sensitive data. The quality routing section discusses the importance of routing in WSNs, challenges, and different routing protocols. Finally, the conclusion section summarizes key points and future directions for achieving secure and efficient WSNs.

3. IMPORTANCE OF WSN

WSNs are pivotal for monitoring various environments like farms and underwater ecosystems (Lilhore, U.K., et. al., 2022) [13], as well as enabling remote patient monitoring in healthcare, but their integration into the Internet of Things (IoT) poses security challenges, addressed by blockchain technology can be implemented to enhance WSN security (Rehman, A., et. al., 2022) [6]. WSNs are crucial for data collection, facing challenges like energy efficiency and coverage. Despite ongoing research, no universal solution exists due to diverse applications, necessitating a comprehensive classification approach, as emphasized by Amutha, J., et. al., 2020 [20]. WSNs' advantages are highlighted in Patidar, Y., et. al., 2024 [14] which include simplified installation, scalability, flexibility, and real-time data monitoring, which enhance decision-making processes. However, they also identify critical issues such as limited battery life, short communication ranges, low processing power, and security vulnerabilities, particularly in remote or sensitive applications (Kaur, P., et. al., 2024) [21].

4. ROUTING PROTOCOLS

4.1 Different Routing Protocols

1. Multipath based protocol

Multipath based protocols establish multiple routes between the source and destination to improve fault tolerance, load balancing, and bandwidth utilization. By using multiple paths, they can enhance the overall reliability and performance of the network.

2. Heterogeneity-based protocol

Heterogeneity based protocols are designed to operate in networks with heterogeneous nodes that have different capabilities such as varying energy levels, processing power, and communication range. They aim to optimize the overall network performance by considering these differences.

3. Location-based protocol

Location based protocols use the geographic positions of nodes to make routing decisions. They often rely on GPS or other positioning systems to determine the most efficient path for data transmission, which can reduce latency and improve energy efficiency.

4. Data-centric protocol

Data-centric protocols focus on the data being transmitted rather than the network topology. These protocols employ techniques such as data aggregation and dissemination to optimize data collection and reduce redundancy, which is particularly useful in sensor network.

5. Hierarchical protocol

Hierarchical protocols organize the network into hierarchical layers, often involving clustering nodes into groups with cluster heads that manage communication within and outside the cluster. This structure helps in scaling the network and reducing energy consumption.

6. Mobility-based protocol

Mobility-based protocols are designed to handle node mobility in dynamic network environments. They adapt to changes in the network topology caused by node movement, ensuring robust and reliable communication.

7. Quality of service-based protocol

Quality of service-based protocols prioritize network resources to meet specific QoS requirements such as bandwidth, delay, jitter, and packet loss. They are crucial for applications that require guaranteed performance levels. Table 1 shows the various categories of routing protocols and their existing routing techniques for WSNs. Figure 1 depicts the various types of routing protocols in WSNs.

Table -1: Existing routing strategies for WSN

Routing Protocols	Routing Techniques	References
Multipath-based Protocols	QoS-driven ad hoc on-demand distance vector (QAODV) routing algorithm for WSNs, utilizing Braided Multipath Routing to enhance the standard AODV with power constraints.	Avudaiammal, R., et. al., 2022 [22]
Heterogeneity-based Protocols	CHR protocol for sensor networks uses low-power L-sensors for data collection and high-end H-sensors for processing and long-range communication, forming clusters for efficient data routing to a central sink.	Brijbhushan, S.A., 2014 [23]
Location-based Protocols	Enhanced Geographical Energy-Aware Routing in Wireless Sensor Networks, Utilizing Node Positioning via GPS for Optimized Data Transmission and Improved Network Performance.	Priyadarshi, R., et. al., 2019 [17]
	BVGF prioritizes short paths but can lead to uneven energy depletion as it doesn't consider remaining sensor energy and some nodes may only have one forwarding option.	Kumar, A., et. al., 2017 [24]
Data-centric Protocols	Efficient Image Retrieval in Mobile Ad Hoc Networks Using SPIN-IT Protocol Based on Metadata Queries	Woodrow, E., et. al., 2002 [25]
	Energy-Aware Data-Centric (EAD) Routing Algorithm tackles energy efficiency through data aggregation, strategic deactivation of leaf nodes, and a dynamic backbone, leading to extended network lifetime compared to traditional and existing energy-aware protocols.	Boukerche, A., et. al., 2005 [26]
Hierarchical Protocols	Energy-Aware Routing Protocol for Wireless Sensor Networks, Leveraging LEACH and Its Descendants for Enhanced Energy Sustainability	

		Kandris, D., et. al., 2023 [19]
	Enhanced Hybrid Energy-Efficient Distributed (EHEED), a multi-sink approach with strategic placement and a more robust cluster head selection method to improve energy efficiency and network performance in WSNs for IoT applications.	Nam, Y., et. al., 2023 [27]
Mobility-based Protocols	Secure Efficient Ad hoc Distance vector (SEAD) offers robust protection against attacks while being efficient for resource-constrained devices. Its design shows promise for enhancing security in these dynamic wireless networks.	Hu, Y.C., et. al., 2003 [28]
Quality of service (Qos)-based Protocols	MMSPEED guaranteed data delivery quality offering multiple speed options for timeliness and used multipath forwarding for reliability. This localized decision-making approach improved network capacity for handling data flows with both requirements.	Felemban, E., et. al., 2006 [29]
	Optimizing SAR in Wireless Body Area Networks Using Particle Swarm Optimization Algorithm for Relay Node Placement.	Wu, T.Y., et. al.,2014 [30]

4.2 Importance of Quality Routing and Routing Challenges

WSNs are a fundamental component of the IoT, driving extensive research into WSN routing protocols. Traditional routing methods often struggle to fully utilize available information, leading to issues like slow communication, poor adaptability to network topology changes and reduced network lifespan (Yang, X., et. al., 2024) [31]. IoT applications such as healthcare, environmental monitoring and defense demand standardization and real-time data collection. In this context, WSNs serve as a critical infrastructure platform for these key applications. However, sensor nodes in WSNs are limited in resource management, storage, communication, and computational capabilities (Roberts, M.K., et. al., 2023) [15].

Designing routing protocols for WSNs primarily aims to extend the network's lifespan by optimizing the use of the limited battery power of sensor nodes (Tan, N.D., et. al., 2023) [32]. Due to the limited power of individual sensor nodes, WSNs require power-saving techniques. Clustering is an effective method that groups nodes together to reduce the transmission distance between sensors and the base station. This approach conserves energy and enhances the network's overall longevity (Dogra, R., et. al., 2023) [16].

Energy efficiency is a major concern in WSNs due to the limited battery life of sensor nodes. Effective management of energy resources is crucial to extend the network's operational lifespan. Routing protocols play a vital role in minimizing energy consumption during data transmission and processing. Several strategies exist to tackle this challenge including clustering, data aggregation, and energy-aware routing algorithms. Clustering protocols such as LEACH, group sensor nodes into clusters. A designated cluster head within each cluster communicates with a central base station. This clustering technique reduces energy consumption by efficiently distributing tasks among nodes. LEACH protocol highlighted by Verma, S., et. al., 2022 [33] enhances energy efficiency significantly by rotating the cluster head role within a network among different nodes. Energy-aware routing protocols, such as the Energy-Efficient and Secure Routing Protocol (EESRP), prioritize selecting routes based on energy metrics to ensure minimal energy consumption. Kim, H.S., et. al., 2023 [34] explored energy-efficient routing protocols by highlighting the significance of selecting paths that consume the least amount of energy.

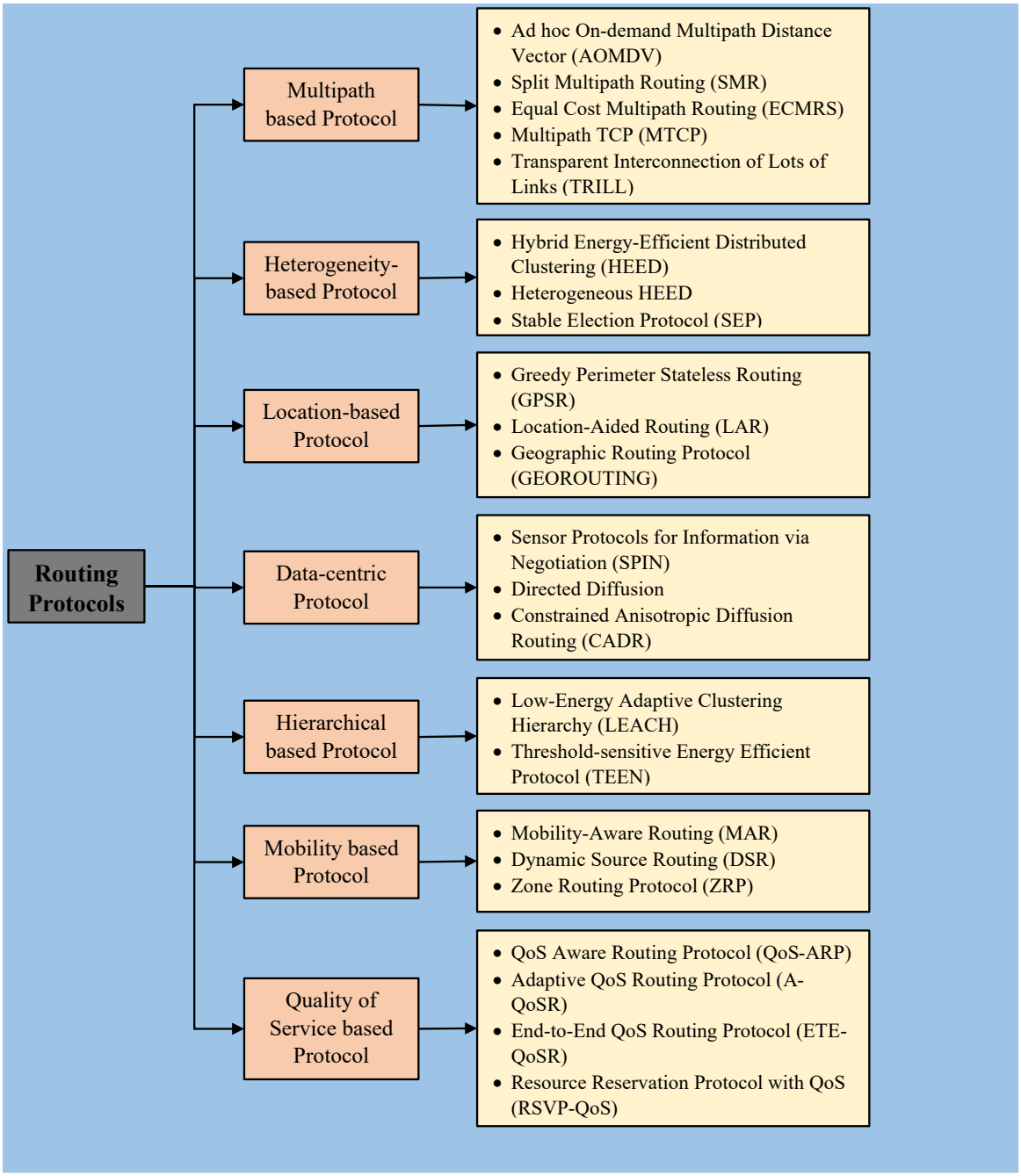

Fig -1: Various Types of Routing Protocols

As WSNs scale up, ensuring efficient routing becomes increasingly complex. Scalability issues arise due to the growing number of nodes. Zone-based protocols like the Zone Routing Protocol (ZRP) handle scalability challenges by dividing the network into zones, reducing routing overhead and improving scalability. Gupta, K., et. al., 2023 [35] discuss recent trends and challenges in zone routing protocols, focusing on enhancing scalability and reducing routing overhead. Network dynamics pose another challenge as WSNs operate in environments where network topology can change frequently. Adaptive routing protocols, such as the

Adaptive Secure and Efficient Routing Protocol (ASERP), dynamically select efficient routes based on current network conditions to maintain performance and reliability. Multi-hop routing strategies allow data to be relayed through intermediate nodes, distributing the energy load and enhancing network longevity. Recent advancements in neural network-based routing enable intelligent protocols to adapt to dynamic network conditions in real-time, optimizing routing decisions and maintaining robust communication paths (Zhou, Q., et. al., 2024) [36].

5. SECURITY CHALLENGES AND THEIR IMPACT

WSNs have a significant impact on fields such as industrial automation, environmental monitoring, etc. However, their open communication channels, limited processing power, and unattended deployment environments make them vulnerable to security attacks. These attacks can have severe consequences for the integrity of collected data, the functionality of the network itself, and the overall reliability of the WSN system.

5.1 WSN Security Attacks

WSN attacks (Faris, M., et. al., 2023) [3], (Yu, J.Y., et. al., 2020) [37] target different layers of the network protocol stack, each with its consequences. Physical layer attacks exploit physical access to nodes or disrupt the radio channel. The data link layer attacks target how data is framed and transmitted, disrupting communication or exhausting the resources. Network layer attacks manipulate routing protocols and data forwarding, leading to compromised data integrity, disrupted routing, or denial-of-service attacks. Transport and application layer attacks target higher-level communication and functionalities, disrupting application-level communication or corrupting the data. By understanding these diverse attack vectors, developers and users of WSNs can take the necessary steps to secure their systems and ensure reliable data collection.

5.1.1 Physical layer attack

Physical attacks (Yu, J.Y., et. al., 2020) [37] on WSNs can cause direct damage to sensors or nodes or interference with their radio communication. These attacks are harder to defend against than software attacks due to the unique characteristics of WSNs, such as their large number of nodes, deployment in challenging environments, and limited processing power. Side channel attacks, jamming attacks, node tampering attacks, camouflage, node replication, node capture, and tampering are also physical layer attacks. Side Channel Attack (SCA) (Nassiri Abrishamchi, M.A., et. al., 2022) [38] exploits leak in encryption such as variations in power consumption and timing, to steal secret keys in resource-limited WSNs. Jamming attack (Del-Valle-Soto, C., et. al., 2021) [39] disrupts communication by flooding the network with noise, resulting in a low signal-to-noise ratio and making it difficult for nodes to transmit data efficiently. Camouflage attack (Santhi, G., et. al., 2017) [40] involves an attacker secretly inserting a malicious node into the WSN which disrupts routing by providing false information while appearing to be a legitimate sensor. Node replication, attackers physically access and replicate nodes, causing wormhole attacks, denial of service, jamming and packet loss, which compromise network confidentiality, integrity, and availability (Anitha, S., et. al., 2021) [41]. Node capture attack (Bhatt, R., et. al., 2020) [42] duplicates a legitimate node's identifier to insert a forged node, allowing communication and eavesdropping, threatening network functions like routing and resource allocation. In tampering attacks, physical access allows attackers to tamper with sensor nodes, compromising sensitive data like keys.

5.1.2 Data link layer attack

The WSN link layer is responsible for framing, error management, and detecting data frames and access. Common attacks that target this layer are traffic analysis, collisions, sleep deprivation, resource depletion, unfairness, and unequal channel allocation (Hasan, M.Z., et. al., 2023) [7]. Traffic analysis in WSNs infers communication patterns by eavesdropping on node interactions (Ebrahimi, Y., et. al., 2022) [8]. In hostile environments, compromised nodes disrupt networks by causing collisions with noise packets. This low-energy, hard-to-trace attack needs robust intrusion and anomaly detection. The exhaustion attack is a type of attack that repeatedly attempts to overload a network's nodes by sending numerous collision requests until the nodes' energy is exhausted. The unfairness attack disrupts authorized access by manipulating node connection periods causing missed transmission deadlines through collisions or misuse of priority mechanisms. A denial of sleep attack disrupts wireless sensor nodes by continuously sending messages, preventing them from entering sleep mode and increasing power consumption.

5.1.3 Network layer attack

WSNs are vulnerable to various attacks at the network layer that disrupt communication and data collection. These attacks include blackhole attack, grayhole attack, sinkhole attack, wormhole attack, sybil attack, byzantine attack, routing attack, and packet replay attack which pose a significant threat to the proper functioning of WSNs. A blackhole attack (Uthumansa, A., et. al., 2020) [9] tricks sensor nodes into sending data through a malicious node that discards it instead of forwarding, disrupting communication and data collection. Selective forwarding is a type of attack that can also be known as grayhole attack, which is a variation of a blackhole attack where malicious nodes intentionally drop or delay packets, disrupting network communication. In a blackhole attack, a malicious node pretends to be the quickest path and then discards all the data packets sent to it instead of forwarding them. However, selective forwarding, allows a compromised node to selectively deny data. Similar to a blackhole attack, a sinkhole attack targets the network layer in WSNs. An attacker compromises surrounding nodes or the sinkhole itself, creating a highly attractive fake route for data to capture all the information in the WSN. A wormhole attack disrupts communication within a WSN by creating a tunnel between two malicious nodes. Attackers establish a high-bandwidth link between two distant compromised nodes. Unsuspected sensor nodes choose this tunnel for routing data, exposing it to the attacker. Thus, leading to eavesdropping, data manipulation and disrupting network communication.

The Sybil assault is also known as a spoofing attack. A single attacker impersonates multiple sensor nodes, flooding the network with false identities disrupting routing protocols, and allowing the attacker to potentially manipulate data flow or even launch other attacks while hiding behind fake nodes. Byzantine attacks exploit a previously trusted node that has been compromised. To disrupt network communication, attackers can launch denial-of-service (DoS) attacks at the Media Access Control (MAC) layer which involves overwhelming network resources by sending excessive traffic and preventing other devices from sending or receiving data.

Routing assaults are one of the most critical threats to WSNs as they target the network’s routing capabilities. These attacks exploit protocols by poisoning routing tables, flooding the network with fake routes, or manipulating packet paths. This disrupts communication, delays data delivery, or sends information down dead ends, hindering the network's ability to function properly. In a packet replay attack at the network layer, an attacker intercepts data packets traveling between sensor nodes. The attacker might delay or even duplicate the packets before sending them on to the receiver leading to outdated or misleading information being received, disrupting network operations, and potentially causing incorrect decisions based on the data.

5.1.4 Transport layer attack

Transport layer attacks exploit weaknesses in protocols like Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to prevent communication between devices by overwhelming systems with connection requests (SYN flood) or data packets (UDP flood) or steal session IDs to impersonate legitimate traffic or gain unauthorized access. TCP SYN flooding is a type of denial-of-service (DoS) attack that exploits the initial connection setup process which is a three-way handshake between devices using TCP. It can exhaust its resources and prevent legitimate connections from being established by overwhelming a target system with a large number of connection requests. It's not a major concern for resource-constrained WSN as they have limited processing power and use of lightweight protocols. User Datagram Protocol floods are another type of Denial-of-Service (DoS) attack that targets the UDP. UDP is a protocol that doesn't require a persistent connection between the sender and receiver. This makes it faster than TCP but also more vulnerable to attacks. In a UDP flood attack, an attacker sends a massive number of UDP packets to a server, overloading its resources and hindering its ability to serve legitimate traffic or requests (Mahmoodi Khaniabadi, S., et. al., 2023) [43].

Session hijacking (Almuhaideb, A.M., et. al., 2020) [44] is an attack in which an attacker takes over a legitimate session between a client and a server. It's done by sniffing network traffic to capture the session ID or other authentication tokens. Once the attacker has the necessary information, they impersonate the client and communicate with the server. Desynchronization attack targets the coordination between sensor nodes constantly disrupting the communication by sending requests to establish connections with one or both nodes which throws the established connection out of sync, preventing them from exchanging data effectively.

5.1.5 Application layer attack

One major security challenge is application layer attacks, where malicious actors target vulnerabilities in the software programs running on the sensor nodes. Application layer attacks, such as DoS, Distributed Denial-of-Service (DDoS), and SQL injection, can disrupt data collection, manipulate sensor readings, or even render the entire network unusable (Subramani, S., et. al., 2023) [45]. Distributed Denial-of-Service (DDoS) attacks the website or service with flood of traffic, making it unavailable to legitimate users. Denial-of-Service (Elsadig, M.A., 2023) [46], similar to DDoS, comes from a single source instead of a distributed network to flood the system with traffic. SQL Injection attacks (Wang, Y.C., et. al., 2023) [47] exploits weaknesses in website forms to inject malicious code into a database disguised as regular input which can steal information, change data, or even crash the database. Table 2 provides a comparison of various common security threats faced by WSNs and the existing countermeasures used to mitigate them.

Table -2: Various security threats and their existing countermeasures

Attack	Existing Solution	References
Jamming attacks	Energy-based Jamming Detection identified abnormal energy depletion in nodes, signaling potential jamming attacks. Compatible with various clustering protocols like PEGASIS, Threshold-sensitive Energy Efficient Protocol (TEEN), Low-Energy Adaptive Clustering Hierarchy (LEACH), and HPAR.	Del-Valle-Soto, C., et. al., 2021 [39]
Node replication	Exponential Moving Average based Replica Detection (EMABRD), Secured Ant Colony Optimization (SACOP) and Fingerprint based Zero Knowledge	Anitha, S., et. al., 2021 [41]

	Authentication (FZKA) detected and prevented attacks in WSNs ensuring the integrity and reliability of the collected data.	
Node capture	Fruit Fly Optimization Algorithm (FFOA) to strategically target these attacks prioritizing nodes with high key value and minimal energy cost for the attacker.	Bhatt, R., et. al., 2020 [42]
Tampering	Swarm Intelligence based defense technique where data packets adapt their unicast or broadcast routing based on channel availability to evade attackers, improving packet delivery and network performance.	Sudha, I., et. al., 2023 [48]
Traffic analysis	Energy-aware scheme to reduce overhead near the base station and cross layer technique to confuse attackers with dynamic data paths, improving anonymity and network lifetime.	Ebrahimi, Y., et. al., 2022 [8]
Collision	Fractional Artificial Bee Colony (FABC) for cluster head selection, Lion Crow Search Optimizer (LCSO) trained Deep Recurrent Neural Network (DRNN) for collision detection, and Dolphin Ant Lion Optimizer (DALO) for pre-scheduling to avoid collisions.	Khare, A., et. al., 2023 [49]
Exhaustion	Detection method based on an energy consumption model to identify abnormal energy usage patterns and potential battery exhaustion attacks.	Shakhov, V.V.,2013 [50]
Denial of sleep attack	Abnormal Sensor Detection Accuracy (ASDA-RSA) a two-phase method using clustering, cryptography, and authentication to improve throughput, packet delivery, network lifetime, and energy efficiency.	Fotohi, R., et. al., 2020 [51]
Blackhole attack	Deep learning system using LSTM to detect Black Hole and Wormhole attacks employed an improved Whale Optimization Algorithm finding optimal paths that bypass these attacks, ensuring secure communication.	Pawar, M.V., 2023 [52]
Wormhole attack	Distributed network discovery approach identified and isolated malicious nodes mitigating nearly all wormhole attack overloads even with a high percentage of compromised nodes.	Modirkhazeni, A., et. al.,2011 [53]

5.2 Existing Security Solutions and Techniques

Securing communication lines involves a combination of encryption, authentication, and access control mechanisms to safeguard data in transit. Encryption makes data unreadable, keeping it confidential. Symmetric encryption uses a single secret key for both encryption and decryption. Symmetric algorithms use Advanced Encryption Standard (AES) which is known for its efficiency. Asymmetric encryption uses a key pair, a public key for encryption and a private key for decryption. Asymmetric algorithms use Elliptic Curve Cryptography (ECC) (Urooj, S., et. al., 2023) [54] and RSA. End-to-end encryption (E2EE) ensures that data is encrypted on the sender's device and can only be decrypted on the recipient's device, thereby preventing intermediaries from accessing the information.

Message integrity and authenticity are confirmed through authentication. Digital signatures are often used with asymmetric encryption, using cryptographic signatures to confirm the sender's identity and prevent message tampering. Message Authentication Codes (MAC) (Zhai, Z., et. al., 2022) [55] authenticate messages using symmetric keys, ensuring data integrity and origin authenticity. Additionally, to authenticate users on a network like comparing IDs, certificate-based authentication depends on trusted Certificate Authorities (CAs). Certificate-based aggregate signatures (CBAS) combine signatures from

multiple sensors into a single compact signature (Zhu, F., et. al., 2021) [56], reducing communication overhead while verifying data authenticity. Unauthorized access to data is limited via access control. Access Control Lists (ACLs) define user access privileges for particular resources, while Role-Based Access Control (RBAC) (Misra, S., et. al., 2011) [57] assigns permissions based on user roles. For increased security, Two-Factor Authentication (2FA) (Chander, B., et. al., 2023) [58]and Multi-Factor Authentication (MFA) require users to provide multiple forms of identification, such as passwords combined with biometrics or one-time codes.

Implementing these techniques effectively requires following best practices. Robust key management involves a storage, distribution, secure generation, and rotation of encryption keys. Secure communication protocols like Transport Layer Security (TLS) or Internet Protocol Security (IPSec) are essential for safeguarding web-based or network-level security respectively. System configuration should stick to industry standards for encryption, authentication, and access control. Regular auditing, monitoring, updates, and patching are crucial to identify and address vulnerabilities and suspicious activities. Because of their limited resources, WSNs have unique security requirements. Several protocols and algorithms have been developed to address these limitations. For instance, TinySec (Rohman, M., et. al., 2023) [59]is a link-layer security protocol that leverages symmetric key cryptography and Message Authentication Codes to provide confidentiality, integrity, and authentication. Localized Encryption and Authentication Protocol (LEAP) focuses on secure communication in clustered WSNs, utilizing localized key management for secure data transmission within clusters.

To achieve a balance between security and energy efficiency, Secure and Energy-Efficient Communication Protocol (SEEC) uses lightweight encryption and authentication mechanisms. Security Protocols for Sensor Networks (SPINS) (Atwal, S., et. al., 2023) [60], (Gaur, A., et. al., 2019) [61] a suite of security protocols for resource-constrained environments consists of two main protocols. Sensor Network Encryption Protocol (SNEP) for lightweight link-layer encryption protocol for data confidentiality and integrity using symmetric cryptography and micro–timed Efficient Streaming Loss-tolerant Authentication (μTESLA) for secure time synchronization and data authentication. A trusted base station is used to ensure the efficient establishment and revocation of keys through the use of the Authenticated Sensor Assisted Protocol (ASAP), a key management protocol. Directed Diffusion with Security (DDS) enhances the Directed Diffusion routing protocol with security features for mitigating various attacks in WSNs. Localized Key Management with Hash Chains (LKH) establishes and distributes keys securely within clusters using hash chains.

To protect against various attacks, LEACH with Enhanced Security (LEACH-ES) incorporates encryption, authentication, and secure data aggregation into the LEACH routing protocol. Datagram Transport Layer Security (DTLS) is a lightweight version of TLS designed for WSNs that provides end-to-end security for communication between sensor nodes and base stations. By deploying these secure communication protocols, WSNs can address various security requirements and protect sensitive data transmitted within the network. Table 3 shows the various existing security solutions and techniques suitable for wireless sensor networks.

Table -3: Existing Security Solutions for WSNs

Existing Security Solutions	Reference
Used a combination of Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) for data encryption and decryption integrated clustering using the LEACH protocol.	Urooj, S., et. al., 2023 [54]
Used link layer protocols, LEACH for clustering and TinySec security for balancing energy efficiency and security.	Rohman, M., et. al., 2023 [59]
Message Authentication Codes (MAC) based authentication to secure relay nodes against energy attacks and replay attacks with low resource usage.	Zhai, Z., et. al., 2022 [55]
Identity-Based Signature Scheme (ISBS) with message recovery enabled secure message broadcasting without sending the original signed message, reducing communication costs.	Feng, M., et. al., 2020 [62]
Two-Factor Authentication (2FA) method using ECC and biometrics, addressed the limitations of existing protocols and enhanced data security in the IoT.	Chander, B., et. al., 2023 [58]
Role-Based Access Control (RBAC) system improved security and throughput in WSNs with unattended nodes.	Misra, S., et. al., 2011 [57]
Certificate-Based Aggregate Signature allowed users to anonymously transmit data while ensuring its authenticity and preventing tampering.	Zhu, F., et. al., 2021 [56]
Lightweight Security Algorithm (LSA) combined with Secure IoT (SIT) algorithm along with the Security Protocols for Sensor Networks (SPINS) security protocol to improve data security while reducing power consumption in WSNs.	Mahlake, N., et. al., 2023 [63]
SPIN protocol, a data-centric routing solution tackled data implosion and overlapped issues by selectively disseminating information only to interested nodes.	Gaur, A., et. al., 2019 [61]

6. PRIVACY-PRESERVING APPROACHES

Privacy is essential in WSNs, ensuring data reaches only its correct destination, preserving user anonymity, complying with regulations, maintaining trust, preventing data leakage, and minimizing exposure, thereby securing the network and its applications. These techniques include secure aggregation, differential privacy, phantom routing, fake packet injection, directional communication mechanisms, random walk, isolation mechanisms, ring routing, and authentication mechanisms (Tripathi, P., et. al., 2019) [64].

However, data aggregation introduces data leakage risks (Qi. X., et. al., 2020) [10] emphasizing secure aggregation, ensuring energy efficiency and network security through end-to-end encryption and hop-by-hop verification. In WSNs, Differential privacy (Jiang, H., et. al., 2020) [11] safeguards sensitive data by concealing individual contributions to datasets, ensuring privacy during collection and analysis. The phantom routing techniques (Chen, Y., et. al., 2022) [12] are used to enhance Source Location Privacy (SLP) by creating uncertainty about the actual source of data packets. Phantom nodes alleviate the protection of SLP to some extent. Fake packet routing (Mutalemwa, L.C., et. al., 2020) [65] strategies, used in cloud-based multi-sink protocols, employ decoy nodes that send packets along with real data to confuse attackers and protect the true source location. A directional communication experiment (Zhang, Y., et. al., 2024) [66] using the Rotating Permanent Magnet Antenna (RPMA) array and a magnetometer is conducted across concrete walls. Random Walk (RW) (Maurya, M.K., et. al., 2022) [67] efficiently routes data

packets by randomly forwarding them between nodes in WSNs, aiding in load balancing but potentially increasing latency. Isolation mechanisms (Wang, Z., et. al., 2021) [68] reduce energy usage in sensor nodes providing efficient transmission, fast response, and enhanced security in wireless sensor networks. Ring routing (Mohapatra, S., et. al., 2023) [69] efficiently connects nodes and sinks, enhancing network performance with minimal overhead. Table 4 shows various existing privacy preserving techniques in WSNs.

Table -4: Privacy preserving techniques in WSN

Key Privacy Preserving Techniques	Reference
A ECC scheme with optimized key management, privacy homomorphism for encryption and rotational MAC for verification, achieved lower energy consumption and higher security.	Qi, X., et. al., 2020 [10]
Differential privacy protected user data in statistical analysis by adding noise to the results.	Jiang, H., et. al., 2020 [11]
Protection Scheme based on Sector Phantom Routing enhanced Source Location Privacy in WSNs by optimizing phantom node placement and routing strategies.	Chen, Y., et. al., 2022 [12]
Directional communication using RPMA arrays improved data collection and pipeline monitoring in underground environments.	Zhang, Y., et. al., 2024 [66]
Cluster-Based Smart Random Walk (CBSRW) routing protocol improved both network lifetime and data delivery efficiency.	Maurya, M.K., et. al., 2022 [67]
Double-layered isolation system using an improved Dijkstra algorithm to find optimal nodes, reducing energy consumption while improving security and response speed.	Wang, Z., et. al., 2021 [68]
Mobile sinks in a ring routing pattern efficiently transferred data, reduced delays and extended network lifetime by minimizing communication overhead.	Mohapatra, S., et. al., 2023 [69]
A detection method using Merkle Hash Trees that identified malicious nodes launching fake packets or selectively dropping packets, improving detection accuracy and packet delivery rates.	Khalid, W., et. al., 2023 [70]

7. DISCUSSION

Wireless Sensor Networks serve as foundational infrastructures for numerous applications from environmental monitoring to healthcare and defense surveillance. This survey paper covers various critical aspects of WSNs by analysing a total of 54 papers across different topics. 5 research papers emphasize the crucial role of WSNs in diverse fields, including environmental monitoring, healthcare, and smart city development. These networks provide real-time data collection, enabling informed decision-making and operational efficiency across various sectors. Quality routing protocols, which are essential for efficient and reliable data transmission in WSNs, are discussed in 15 papers. This area focuses on developing protocols that adapt to dynamic network conditions, ensure reliable data delivery, and mitigate routing attacks. The variety of protocols studied includes multipath, hierarchical and mobility-based approaches, each tailored to specific network characteristics and application requirements. These protocols address challenges such as energy efficiency, network lifetime, and scalability. Security challenges and existing solutions constitute the most substantial section with 27 papers, reflecting the critical need to protect WSNs from various threats such as data breaches, tampering, and denial-of-service attacks. This section concentrates on developing robust security mechanisms such as encryption, authentication, intrusion detection systems, and secure

routing protocols. Addressing these challenges is crucial to safeguarding sensitive data and ensuring the reliability and trustworthiness of WSN deployments. Privacy-preserving techniques are covered in 7 papers, focusing on methods to protect sensitive information and maintain user anonymity within WSNs. These techniques include secure aggregation, differential privacy, phantom routing, and authentication mechanisms. This section explores methods to enhance data confidentiality and prevent unauthorized access, considering the resource constraints and operational challenges unique to sensor networks.

This survey offers a thorough analysis of cutting-edge WSN research, covering crucial aspects like routing protocols, security challenges, and privacy techniques, paving the way for wider adoption and integration within IoT ecosystems. In the realm of security, the secure and energy-efficient communication protocol emerges as a formidable choice. By striking a delicate balance between security and energy efficiency, SEEC addresses the multifaceted challenges posed by diverse attack vectors in WSNs. Leveraging lightweight encryption and authentication mechanisms such as symmetric cryptography and MAC. SEEC ensures the confidentiality, integrity, and authenticity of data transmission within the network. Its efficacy extends to thwarting physical layer attacks like jamming and node replication, as well as data link layer attacks such as traffic analysis and resource exhaustion. Furthermore, SEEC's energy-efficient design renders it highly suitable for resource-constrained environments, enabling WSNs to uphold robust security measures without sacrificing performance or consuming excessive power.

Complementing the robust security framework, privacy-preserving techniques play a pivotal role in safeguarding sensitive data within WSNs. Among these techniques, differential privacy emerges as a beacon of effectiveness. Its foundation on strong theoretical principles enables it to provide rigorous privacy guarantees by introducing noise or randomness to query responses. This proactive approach ensures that individual data contributions do not unduly influence the outcome of analyses, thereby mitigating the risk of privacy breaches. Unlike ad-hoc methods such as data masking or anonymization, differential privacy offers a mathematically rigorous framework that remains resilient against various types of attacks, including inference and linkage attacks. Its scalability and compatibility with diverse data analysis techniques further solidify its position as a versatile and robust privacy-preserving solution for WSNs.

Quality routing stands as another cornerstone in the efficient operation of WSNs, directly influencing their reliability, efficiency, and longevity. LEACH protocol exemplifies excellence in this domain with its energy-efficient clustering approach. By dynamically rotating the cluster head role among nodes, LEACH optimizes energy utilization, thereby prolonging the operational lifespan of the network. This approach not only minimizes energy consumption but also enables the network to adapt to dynamic changes in topology, ensuring seamless communication and preserving data integrity.

8. CONCLUSION

This paper explored the three core components of WSNs, security solutions, privacy-preserving techniques, and quality routing protocols. It examined their significant impact on WSN's efficiency and reliability. SEEC emerged as a compelling solution for WSN security, offering a balanced approach between robust protection and energy efficiency. Differential privacy stood out as a powerful privacy-preserving technique, guaranteeing data anonymity through strong theoretical foundations. Lastly, the LEACH protocol demonstrated excellence in routing efficiency, enabling seamless communication and extending network lifespan through its dynamic clustering approach. Together, these components form a comprehensive framework for safeguarding WSNs and supporting their diverse applications across various domains. By

integrating robust security mechanisms, proactive privacy-preserving techniques, and efficient routing protocols.

WSNs can effectively address the multifaceted challenges they face, ensuring reliability, efficiency, and longevity. However, it is crucial to acknowledge potential trade-offs. Security measures like encryption can consume additional power, impacting routing efficiency. Similarly, privacy-preserving techniques like differential privacy might introduce noise that affects data accuracy. Therefore, WSN design necessitates careful consideration of these interactions to achieve an optimal balance between security, privacy, and routing performance.

By prioritizing this multifaceted approach, we can empower WSNs to reach their full potential and revolutionize data collection across various sectors. Future research could further explore the interplay between emerging technologies and WSN security, privacy, and routing, paving the way for innovative solutions and enhanced network resilience.

REFERENCES

[1] Kizza, J.M., 2024. Security in Sensor Networks. In Guide to Computer Network Security (pp. 475-490). Cham: Springer International Publishing.
[2] Adil, M., Menon, V.G., Balasubramanian, V., Alotaibi, S.R., Song, H., Jin, Z. and Farouk, A., 2022. Survey: Self-Empowered Wireless Sensor Networks Security Taxonomy, Challenges, and Future Research Directions. IEEE Sensors Journal, 23(18), pp.20519-20535.
[3] Faris, M., Mahmud, M.N., Salleh, M.F.M. and Alnoor, A., 2023. Wireless sensor network security: A recent review based on state-of-the-art works. International Journal of Engineering Business Management, 15, p.18479790231157220.
[4] Kandris, D., Nakas, C., Vomvas, D. and Koulouras, G., 2020. Applications of wireless sensor networks: an up-to-date survey. Applied system innovation, 3(1), p.14.
[5] Alansari, Z., Anuar, N.B., Kamsin, A. and Belgaum, M.R., 2022. A systematic review of routing attacks detection in wireless sensor networks. PeerJ Computer Science, 8, p.e1135.
[6] Rehman, A., Abdullah, S., Fatima, M., Iqbal, M.W., Almarhabi, K.A., Ashraf, M.U. and Ali, S., 2022. Ensuring security and energy efficiency of wireless sensor network by using blockchain. Applied Sciences, 12(21), p.10794.
[7] Hasan, M.Z., Hanapi, Z.M. and Hussain, M.Z., 2023. Wireless Sensor Security Issues on Data Link Layer: A Survey. Computers, Materials & Continua, 75(2).
[8] Ebrahimi, Y. and Younis, M., 2022. Energy-aware cross-layer technique for countering traffic analysis attacks on wireless sensor network. IEEE Access, 10, pp.131036-131052.
[9] Uthumansa, A. and Shantha, F., 2020. Identifying the impacts of active and passive attacks on network layer in a mobile ad-hoc network: a simulation perspective.
[10] Qi, X., Liu, X., Yu, J. and Zhang, Q., 2020. A privacy data aggregation scheme for wireless sensor networks. Procedia Computer Science, 174, pp.578-583.
[11] Jiang, H., Pei, J., Yu, D., Yu, J., Gong, B. and Cheng, X., 2020. Differential privacy and its applications in social network analysis: A survey. arXiv preprint arXiv:2010.02973.
[12] Chen, Y., Sun, J., Yang, Y., Li, T., Niu, X. and Zhou, H., 2022. PSSPR: a source location privacy protection scheme based on sector phantom routing in WSNs. International Journal of Intelligent Systems, 37(2), pp.1204-1221.
[13] Lilhore, U.K., Khalaf, O.I., Simaiya, S., Tavera Romero, C.A., Abdulsahib, G.M. and Kumar, D., 2022. A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks. International Journal of Distributed Sensor Networks, 18(9), p.15501329221117118.
[14] Patidar, Y., Jain, M. and Vyas, A.K., 2024. Routing in Wireless Sensor Networks and Internet of Things: Systematic Analysis and Discussion. In AIoT and Smart Sensing Technologies for Smart Devices (pp. 181-196). IGI Global.
[15] Roberts, M.K. and Ramasamy, P., 2023. An improved high performance clustering based routing protocol for wireless sensor networks in IoT. Telecommunication Systems, 82(1), pp.45-59.

[16] Dogra, R., Rani, S. and Gianini, G., 2023. REERP: a region-based energy-efficient routing protocol for IoT wireless sensor networks. Energies, 16(17), p.6248.
[17] Priyadarshi, R., Soni, S.K. and Sharma, P., 2019. An enhanced GEAR protocol for wireless sensor networks. In Nanoelectronics, Circuits and Communication Systems: Proceeding of NCCS 2017 (pp. 289-297). Springer Singapore.
[18] Olivia, D., Nayak, A. and Balachandra, M., 2021. Data-centric load and QoS-aware body-to-body network routing protocol for mass casualty incident. IEEE Access, 9, pp.70683-70699.
[19] Kandris, D., Evangelakos, E.A., Rountos, D., Tselikis, G. and Anastasiadis, E., 2023. LEACH-based hierarchical energy efficient routing in wireless sensor networks. AEU-International Journal of Electronics and Communications, 169, p.154758.
[20] Amutha, J., Sharma, S. and Nagar, J., 2020. WSN strategies based on sensors, deployment, sensing models, coverage and energy efficiency: Review, approaches and open issues. Wireless Personal Communications, 111(2), pp.1089-1115.
[21] Kaur, P. and Singh, P., 2024. Adaptive Data Transmission Protocols for Energy Harvesting WSNs Used in Agriculture. Journal of Telecommunications and Information Technology, (1), pp.97-103.
[22] Avudaiammal, R., Sowmyaa Vathsan, M.S. and Sivashanmugam, S.O., 2022. QoS-driven AODV algorithm for WSN. In Futuristic Communication and Network Technologies: Select Proceedings of VICFCNT 2020 (pp. 115-125). Springer Singapore.
[23] Brijbhushan, S.A., 2014. A Survey-Wireless Sensor Networks Routing Protocols. International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume, 4.
[24] Kumar, A., Shwe, H.Y., Wong, K.J. and Chong, P.H., 2017. Location-based routing protocols for wireless sensor networks: A survey. Wireless Sensor Network, 9(1), pp.25-72.
[25] Woodrow, E. and Heinzelman, W., 2002, September. SPIN-IT: a data centric routing protocol for image retrieval in wireless networks. In Proceedings. International Conference on Image Processing (Vol. 3, pp. 913-916). IEEE.
[26] Boukerche, A., Cheng, X. and Linus, J., 2005. A performance evaluation of a novel energy-aware data-centric routing algorithm in wireless sensor networks. Wireless Networks, 11(5), pp.619-635.
[27] Nam, Y., Mugerwa, D., Choi, H., Kwon, Y. and Lee, E., 2023, July. Enhanced Hybrid Energy-Efficient Distributed Clustering Protocol for IoT-Based WSNs with Multiple Sinks. In 2023 IEEE Sensors Applications Symposium (SAS) (pp. 1-6). IEEE.
[28] Hu, Y.C., Johnson, D.B. and Perrig, A., 2003. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad hoc networks, 1(1), pp.175-192.
[29] Felemban, E., Lee, C.G. and Ekici, E., 2006. MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks. IEEE transactions on mobile computing, 5(6), pp.738-754.
[30] Wu, T.Y. and Lin, C.H., 2014. Low-SAR path discovery by particle swarm optimization algorithm in wireless body area networks. IEEE Sensors Journal, 15(2), pp.928-936.
[31] Yang, X., Yan, J., Wang, D., Xu, Y. and Hua, G., 2024. WOAD3QN-RP: An intelligent routing protocol in wireless sensor networks—A swarm intelligence and deep reinforcement learning based approach. Expert Systems with Applications, 246, p.123089.
[32] Tan, N.D. and Nguyen, V.H., 2023. EE-TLT: Energy-efficient routing protocol using two-level tree-based clustering in wireless sensor network. Journal of Communications and Networks, 25(6), pp.734-749.
[33] Verma, S., Bharti, P. K., & Singh, V. P. (2022) 'Energy-efficient clustering and data aggregation in wireless sensor networks', Wireless Networks, Springer.
[34] Kim, H. S., Park, J. H., & Kim, T. (2023) 'A survey of energy-efficient routing protocols for wireless sensor networks', Journal of Network and Computer Applications, Elsevier.
[35] Gupta, K., & Patel, R. (2023) 'Zone routing protocols for wireless sensor networks: Recent trends and challenges', IEEE Communications Surveys & Tutorials.
[36] Zhou, Q., & Wang, Y. (2024) 'Intelligent routing in WSNs using neural networks: A survey', IEEE Transactions on Neural Networks and Learning Systems.
[37] Yu, J.Y., Lee, E., Oh, S.R., Seo, Y.D. and Kim, Y.G., 2020. A survey on security requirements for WSNs: focusing on the characteristics related to security. IEEE Access, 8, pp.45304-45324.
[38] Nassiri Abrishamchi, M.A., Zainal, A., Ghaleb, F.A., Qasem, S.N. and Albarrak, A.M., 2022. Smart home privacy protection methods against a passive wireless snooping side-channel attack. Sensors, 22(21), p.8564.

[39] Del-Valle-Soto, C., Mex-Perera, C., Nolazco-Flores, J.A., Rodríguez, A., Rosas-Caro, J.C. and Martínez-Herrera, A.F., 2021. A low-cost jamming detection approach using performance metrics in cluster-based wireless sensor networks. Sensors, 21(4), p.1179.

[40] G. Santhi and R. Sowmiya, "A survey on various attacks and countermeasures in wireless sensor networks", Int. J. Comput. Appl., vol. 159, no. 7, pp. 7-11, Feb. 2017.

[41] Anitha, S., Jayanthi, P. and Chandrasekaran, V., 2021. An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks. Measurement, 167, p.108272.

[42] Bhatt, R., Maheshwary, P., Shukla, P., Shukla, P., Shrivastava, M. and Changlani, S., 2020. Implementation of fruit fly optimization algorithm (FFOA) to escalate the attacking efficiency of node capture attack in wireless sensor networks (WSN). Computer Communications, 149, pp.134-145.

[43] Mahmoodi Khaniabadi, S., Javadpour, A., Gheisari, M., Zhang, W., Liu, Y. and Sangaiah, A.K., 2023. An intelligent sustainable efficient transmission internet protocol to switch between User Datagram Protocol and Transmission Control Protocol in IoT computing. Expert Systems, 40(5), p.e13129.

[44] Almuhaideb, A.M. and Alqudaihi, K.S., 2020. A lightweight three-factor authentication scheme for WHSN architecture. Sensors, 20(23), p.6860.

[45] Subramani, S. and Selvi, M., 2023. Comprehensive review on distributed denial of service attacks in wireless sensor networks. International Journal of Information and Computer Security, 20(3-4), pp.414-438.

[46] Elsadig, M.A., 2023. Detection of Denial-of-Service Attack in Wireless Sensor Networks: A lightweight Machine Learning Approach. IEEE Access.

[47] Wang, Y.C., Zhang, G.L. and Zhang, Y.L., 2023. Analysis of SQL Injection Based on Petri Net in Wireless Network. Journal of Information Science & Engineering, 39(1).

[48] Sudha, I., Mustafa, M.A., Suguna, R., Karupusamy, S., Ammisetty, V., Shavkatovich, S.N., Ramalingam, M. and Kanani, P., 2023. Pulse jamming attack detection using swarm intelligence in wireless sensor networks. Optik, 272, p.170251.

[49] Khare, A., K, S. and Dugyala, R., 2023. Detection of collision using optimized deep model and mitigation of collision using dolphin ant lion optimizer in wireless sensor network. International Journal of Communication Systems, 36(13), p.e5525.

[50] Shakhov, V.V., 2013. Protecting wireless sensor networks from energy exhausting attacks. In Computational Science and Its Applications–ICCSA 2013: 13th International Conference, Ho Chi Minh City, Vietnam, June 24-27, 2013, Proceedings, Part I 13 (pp. 184-193). Springer Berlin Heidelberg.

[51] Fotohi, R., Firoozi Bari, S. and Yusefi, M., 2020. Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol. International Journal of Communication Systems, 33(4), p.e4234.

[52] Pawar, M.V., 2023. Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. International Journal of Pervasive Computing and Communications, 19(1), pp.124-153.

[53] Modirkhazeni, A., Aghamahmoodi, S., Modirkhazeni, A. and Niknejad, N., 2011, September. Distributed approach to mitigate wormhole attack in wireless sensor networks. In 7th International Conference on Networked Computing (pp. 122-128). IEEE.

[54] Urooj, S., Lata, S., Ahmad, S., Mehfuz, S. and Kalathil, S., 2023. Cryptographic data security for reliable wireless sensor network. Alexandria Engineering Journal, 72, pp.37-50.

[55] Zhai, Z., Lai, G., Cheng, B., Qian, J., Zhao, L., Wu, J. and Wan, Z., 2022. Lightweight secure detection service for malicious attacks in wsn with timestamp-based mac. IEEE Transactions on Network and Service Management, 19(4), pp.5299-5311.

[56] Zhu, F., Yi, X., Abuadbba, A., Khalil, I., Nepal, S., Huang, X. and Yan, X., 2021. Certificate-based anonymous authentication with efficient aggregation for wireless medical sensor networks. IEEE Internet of Things Journal, 9(14), pp.12209-12218.

[57] Misra, S. and Vaish, A., 2011. Reputation-based role assignment for role-based access control in wireless sensor networks. Computer Communications, 34(3), pp.281-294.

[58] Chander, B. and Kumaravelan, G., 2023. An improved 2-factor authentication scheme for WSN based on ECC. IETE Technical Review, 40(2), pp.167-178.

[59] Rohman, M., Yulianto, B., Suprapto, S., Baskoro, F. and Aribowo, W., 2023, April. Work energy modeling link layer protocol on TinyOS and TinySec based wireless sensor networks with LEACH method. In AIP Conference Proceedings (Vol. 2646, No. 1). AIP Publishing.

[60] Atwal, S. and Kamboj, S., 2023. Key Issues And Challenges In Security Protocols (SPINS) For Sensor Network.

[61]Gaur, A. and Verma, M.R., 2019. Survey Paper for SPIN Protocol in Wireless Sensor Network.
[62]Feng, M., Lai, C.F., Liu, H., Qi, R. and Shen, J., 2020. A novel identity-based broadcast authentication scheme with batch verification for wireless sensor networks. Journal of Internet Technology, 21(5), pp.1303-1311.
[63]Mahlake, N., Mathonsi, T.E., Muchenje, T. and Plessis, D.D., 2023. A Hybrid Algorithm to Enhance Wireless Sensor Networks security on the IoT. arXiv preprint arXiv:2303.14445.
[64]TRIPATHI, P., KUMAR, S. and SINGH, V., 2019. Overview of Attacks and Security Threats in Wireless Sensor Networks (WNS). Technological and Managerial Strategies for Next Generation Transformation, p.184.
[65]Mutalemwa, L.C. and Shin, S., 2020. Comprehensive performance analysis of privacy protection protocols utilizing fake packet injection techniques. IEEE Access, 8, pp.76935-76950.
[66]Zhang, Y., Cui, Y., Wang, C., Song, X., Pei, Y. and Yuan, Z., 2024. Rotating permanent magnet antenna array for directional communication in pipeline monitoring system. AEU-International Journal of Electronics and Communications, p.155210.
[67]Maurya, M.K., Shivhare, A., Ali, A., Mishra, A. and Kumar, M., 2022, December. Cluster based smart random walk for data aggregation in wireless sensor network. In 2022 IEEE 15th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC) (pp. 98-104). IEEE.
[68]Wang, Z., Zhang, Q. and Gao, C., 2021. A double-layer isolation mechanism for malicious nodes in wireless sensor networks. Wireless Networks, 27(4), pp.2391-2407.
[69]Mohapatra, S., Behera, P.K., Sahoo, P.K., Ojha, M.K., Swarup, C., Singh, K.U., Pandey, S.K., Kumar, A. and Goswami, A., 2023. Modified ring routing protocol for mobile sinks in a dynamic sensor network in smart monitoring applications. Electronics, 12(2), p.281.
[70]Khalid, W., Ahmad, N., Khan, S., Saquib, N.U., Arshad, M. and Shahwar, D., 2023. FAPMIC: Fake packet and selective packet drops attacks mitigation by Merkle hash tree in intermittently connected networks. IEEE Access, 11, pp.4549-4573.