International Journal of Research in Advent Technology, Vol.13, No.3, September 2025
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Systematic Literature Review on Secure Routing Protocols in Wireless Networks: Current Trends and Future Directions

Peter Maina Mwangi, Juliet Gathoni Muchori

Abstract—Wireless Sensor Networks (WSNs) are increasingly being deployed in a wide range of applications, including environmental monitoring, smart healthcare, industrial automation, and military surveillance. Despite their versatility, WSNs are inherently prone to security threats due to characteristics such as constrained energy resources, open communication channels, and often remote or unattended deployments. These vulnerabilities are especially critical at the routing layer, where attacks such as Sybil, wormhole, blackhole, and selective forwarding can significantly disrupt network operations. To address these challenges, secure routing protocols have been proposed to ensure data integrity, confidentiality, and reliable packet delivery. This paper presents a systematic literature review of secure routing protocols in WSNs, conducted following the PRISMA 2020 guidelines. The review is guided by three central research questions: (1) What are the main attacks in WSNs and the methods/techniques used to mitigate these attacks? (2) What secure routing protocols have been developed for Wireless Sensor Networks, and what are their respective strengths, weaknesses, and areas of application? (3) What strategies that may influence the future design of secure routing protocols in WSNs? A total of 40 peer reviewed publications from 2019 to 2025 were selected from reputable databases including IEEE Xplore, SpringerLink, ScienceDirect, MDPI, Wiley Online Library, and the ACM Digital Library. The analysis reveals a range of attack mitigation strategies and secure routing protocols such as SEARP, ITEERP, ESR, SeRINS, and IASR. Each protocol offers different trade-offs in terms of security robustness, energy consumption, scalability, and adaptability. Furthermore, trends such as artificial intelligence, edge computing, and lightweight cryptographic methods are identified as key drivers for future protocol development. This review looks at current research and outlines areas for future exploration in secure WSN routing.

Index Terms—Ariadne, ESR, IASR, ITEERP, RLEACH, SEAD, SEARP, SeRINS, SRP, Tinysec, Wireless sensor Network (WSNs)

Manuscript received on August 13, 2025, revised on September 15, 2025 and published on September 30, 2025

Peter Maina Mwangi, *Computing and Information Technology Department, Mama Ngina University College and Information Technology Department, Murang'a University of Technology, Kenya.*
Email: pmwangi@mnu.ac.ke
Juliet Gathoni Muchori*, Computing and Information Technology Department, Mama Ngina University College and Information Technology Department, Murang'a University of Technology, Kenya.*
Email: jmuchori@mut.ac.ke

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have become a foundational technology for a wide range of applications, including environmental monitoring, smart agriculture, healthcare, industrial automation, and military surveillance [1], [2], [3]. These networks consist of distributed sensor nodes that are typically small, low-powered, and resource-constrained, designed to sense, process, and transmit data to central locations or sink nodes. The inherent characteristics of WSNs—namely their open communication medium, decentralized control, and energy constraints—pose unique security challenges. In particular, the routing protocols that govern communication in WSNs are highly susceptible to a variety of attacks that can compromise data integrity, availability, and confidentiality [4].

The routing layer in WSNs is often targeted by adversaries because it plays a critical role in ensuring the efficient and accurate delivery of sensor data. Attacks such as wormhole, Sybil, sinkhole, selective forwarding, and hello flood can disrupt the normal operation of the network by dropping packets, injecting false information, or rerouting traffic through malicious nodes [5]. The consequences of such attacks are severe in mission-critical applications like battlefield surveillance or patient health monitoring, where incorrect or delayed data can lead to dire outcomes. Therefore, designing secure routing protocols that can detect and mitigate these threats is essential for the reliability of WSN deployments [6].

To address these vulnerabilities, researchers have proposed a wide variety of secure routing protocols and mitigation techniques. These range from cryptographic solutions that ensure authentication and encryption to trust-based models that evaluate the behavior of nodes over time. Other approaches involve intrusion detection systems, anomaly detection using machine learning, and more recently, blockchain technologies for decentralized trust management. However, each solution comes with trade-offs related to energy consumption, computational overhead, scalability, and ease of deployment. As WSNs are often deployed in hostile or remote environments, these trade-offs must be carefully balanced to maintain operational efficiency without sacrificing security [7], [8].

While several surveys have been conducted in recent years, many are either narrowly focused on specific attacks or lack a systematic review methodology [6], [5] and [9] . A

doi: 10.32622/ijrat.133202511

comprehensive, systematic literature review is needed to critically analyze the current landscape of secure routing in WSNs. Such a review not only synthesizes existing knowledge but also provides a structured framework for comparing the effectiveness, limitations, and applicability of various protocols. Moreover, it can help identify research gaps and highlight promising areas for future investigation, especially as new technologies such as artificial intelligence (AI), edge computing, and quantum cryptography begin to influence the field.

This research seeks to address that requirement by performing a systematic evaluation of secure routing methods in wireless sensor networks (WSNs), adhering to the 2020 Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) standards. The study is organized around three research questions that aim to identify primary security threats in wireless sensor networks (WSNs), evaluate current secure routing protocols, assess their advantages and disadvantages, and investigate emerging technologies poised to influence the future of secure routing solutions. By doing so, the paper provides a current and critical understanding of WSN security and lays the groundwork for future advancements in this rapidly evolving area of research.

II. Related Work

In the last few years, a lot of studies have looked at the security problems and routing methods in Wireless Sensor Networks (WSNs). These reviews have contributed significantly to understanding how various attacks can be launched against sensor networks and how secure routing can be implemented to counter them.

Alabady et al. [10] provided a broad classification of security challenges in WSNs, categorizing them into physical, link layer, network layer, and transport layer threats. They offered detailed descriptions of popular routing attacks such as wormhole, blackhole, and Sybil attacks, and discussed general mitigation strategies including cryptographic techniques, trust-based models, and intrusion detection systems. However, their work, while extensive, lacked depth in evaluating the performance and suitability of specific secure routing protocols under different application scenarios.

Khaled et al. [11] reviewed security challenges and solutions in Wireless Sensor Networks. The goal of the article was to present a thorough understanding of the security issues in WSNs and offer potential fixes that could be used to improve network security. The infrastructure and classifications of WSNs, routing problems, and the categorization of routing protocols in WSNs are all covered in the study. The several kinds of assaults that WSNs are susceptible to, the steps that may be taken to lessen these attacks, and the trust and reputation management systems in WSNs are then highlighted in this overview of security challenges in WSNs. Lastly, the most significant unresolved problems and potential paths for WSN security are examined. The paper systematically categorizes and discusses a wide array of security threats affecting WSNs, including node compromise, eavesdropping, denial-of-service (DoS), and routing attacks like sinkhole and Sybil attacks. This thorough analysis provides readers with a clear understanding of the multifaceted security challenges in WSNs. Although the paper discusses a number of security measures, it does not provide a thorough comparison of certain secure routing systems. The findings' practical application would be improved by thorough analyses of protocol performance measures like energy consumption, latency, and scalability.

Similarly, Boudia and Feham [12] conducted a review specifically focused on trust-based routing protocols. Their analysis emphasized the importance of trust models in detecting malicious behavior, particularly in decentralized networks where centralized control is not feasible. One of the key strengths of their study lies in its classification of trust metrics—such as direct, indirect, and hybrid trust—which can be used to inform secure routing decisions. Nevertheless, the study did not consider recent innovations like blockchain-based trust management or machine learning-assisted routing, limiting its relevance to emerging technological contexts.

Chen et al. [13]explored secure routing protocols in WSNs from a cryptographic perspective. Their review categorized routing solutions into symmetric key, public key, and hybrid schemes. They highlighted protocols such as TinySec and SPINS, which are optimized for energy efficiency and lightweight operations. The major strength of this review is its focus on the energy-security tradeoff, a crucial factor in sensor node deployment. However, it lacked empirical comparisons or a comprehensive evaluation of protocol performance metrics such as latency, throughput, or scalability in real-world scenarios.

In another study, Javed et al. [14] extended the scope by evaluating both routing protocols and their associated vulnerabilities. Their survey presented a taxonomy of routing techniques including flat, hierarchical, and location-based routing. While this taxonomy aids in understanding the functional categorization of protocols, the review does not systematically assess the security enhancements specific to each category. Additionally, the authors acknowledged that their survey lacked a standardized framework such as PRISMA for systematic inclusion and exclusion of studies, which may affect reproducibility and comprehensiveness.

Recent works have attempted to bridge the gap between traditional protocol analysis and future-oriented technologies. For instance, Farooq et al. [15] proposed a blockchain-enabled trust-based routing protocol and discussed its potential in establishing decentralized, tamper-proof security infrastructures. Similarly, Gupta and Singh [16]reviewed the integration of machine learning (ML) in secure routing, noting how predictive models can enhance anomaly detection and adapt routing paths dynamically. These contributions mark a shift towards intelligent and autonomous security models; however, they also raise new concerns related to computational overhead and energy consumption, which are often underexplored in literature.

The lack of a systematic and replicable methodology for the selection and analysis of literature is a major limitation

doi: 10.32622/ijrat.133202511

across many of the reviewed studies, despite these valuable contributions. Most of these studies do not follow systematic review standards like PRISMA, which could lead to biases in the inclusion of studies. Additionally, few works holistically address the intersection of attack mitigation, protocol effectiveness, and future trends like AI, edge computing, and quantum cryptography. This paper attempts to fill these gaps by using PRISMA guidelines to analyze secure routing protocols and current WSN security practices to provide a comprehensive picture of the state and direction of the field.

III. Research Method

The 2020 PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines are followed in this study to ensure a transparent, reproducible, and systematic literature review on secure routing protocols and current security mechanisms in Wireless Sensor Networks (WSNs). The researcher used these standards because they provide a structured framework to systematically identify, assess, and synthesize studies, ensuring comprehensive and unbiased coverage of relevant literature, and because they enforce transparent reporting of how studies are selected, screened, and synthesized, making it easier for others to replicate the review or build upon it [17], [18]. Finally, adhering to PRISMA gives your work more academic rigor and reputation, which increases its publishing ability and reliability in the eyes of the research community. For a given subject, topic area, or phenomenon of interest, a scientific literature review finds, assesses, and interprets pertinent research. Because it focuses on systematic literature reviews, which are regarded as secondary research, this study is categorized as a tertiary literature review. Figure 1 shows the four Phases in this guideline.

A. *Identification*

Step 1: Define the Research Questions

This literature review aims to acquire and evaluate the comprehensive knowledge of secure routing methods in wireless sensor networks (WSNs). By synthesizing existing research, we aim to establish a foundation for future inquiries, provide insights for practitioners to enhance WSN implementations, and inform policymakers of the problems and advancements in this vital aspect of wireless sensor networks. This study enhances the efficiency and security of Wireless Sensor Networks (WSNs), facilitating their further expansion and innovation across several application fields. The study poses numerous research inquiries to provoke conversation. This review is organized around three main research questions:

What are the main attacks in WSNs and the methods/techniques used to mitigate these attacks?

What secure routing protocols have been developed for Wireless Sensor Networks, and what are their respective strengths, weaknesses, and areas of application?

What strategies that may influence the future design of secure routing protocols in WSNs?

Step 2: Develop a Protocol

This step involves designing a clear and structured review protocol. The protocol defines the research questions, target keywords (e.g., "secure routing in WSN", "WSN security attacks", "intrusion detection in WSN"), inclusion and exclusion criteria (such as focusing on papers from 2019 to 2025), and the databases to be searched like IEEE Xplore, SpringerLink, ScienceDirect (Elsevier), MDPI, Wiley Online Library, and ACM. This structured plan helps guide the review process and ensures consistency and objectivity in selecting and analyzing studies. To ensure the relevance and quality of the studies included in the review, the following inclusion and exclusion criteria were defined:

Inclusion Criteria:

Peer-reviewed journal and conference articles published between January 2019 and May 2025.

Studies focusing on secure routing protocols in WSNs, including trust-based, cryptographic, ML-based, or blockchain-based approaches.

Articles addressing attacks and mitigation strategies in the context of WSNs.

Studies written in English.

Exclusion Criteria:

Studies not focused on WSNs (e.g., general IoT, MANETs without WSN context).

Articles not addressing security or routing (e.g., solely on energy efficiency or MAC protocols).

Duplicates, editorials, prefaces, theses, and non-peer-reviewed sources.

Step 3:Search for Studies

A thorough and systematic literature search is performed across selected academic databases to gather relevant articles on secure routing protocols and security mechanisms in WSNs. The search uses predefined keywords and Boolean combinations such as ("WSN" AND "secure routing") OR ("wireless sensor network" AND "security attacks"). This ensures the identification of a wide range of recent and high-quality research papers that contribute to understanding how security threats in WSNs are addressed through routing protocols and other defense techniques. A table has been generated for the years 2019-2025, displaying the academic databases from which papers were reviewed, as well as the quantity of journal papers studied. Table 1 displays papers picked from each academic database.

TABLE 1: LIST OF JOURNAL PAPERS COLLECTED FROM MAJOR ACADEMIC DATABASES.

Academic Databases	No of Journal Papers Reviewed
ScienceDirect (Elsevier)	50
IEEE Xplore	45
ACM Digital library	30
SpringerLink	20
Wiley Online Library	20
MDPI	15
arXiv.	20
Total	200

doi: 10.32622/ijrat.133202511

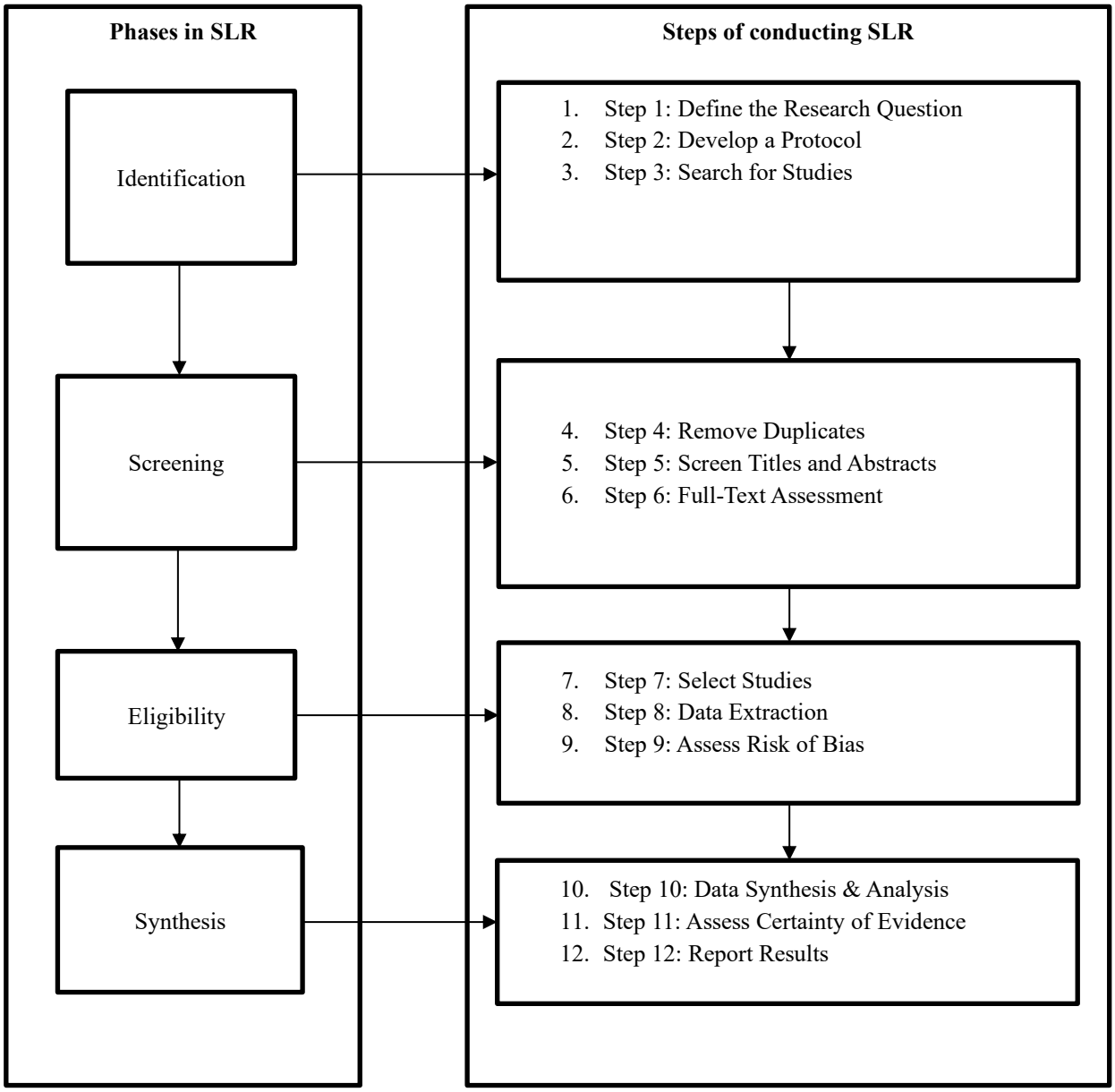

Fig 1: The Phases of PRISMA Guidelines

B. *Screening*

Step 4 Remove Duplicates

After collecting research articles from multiple databases like IEEE Xplore, SpringerLink, ScienceDirect (Elsevier),

MDPI, Wiley Online Library, and ACM, the first task is to remove duplicate records. Since the same paper may appear in more than one source, duplicate removal ensures that each study is only considered once, preventing bias and redundancy in the review process.

Step 5: Screen Titles and Abstracts

Next, the titles and abstracts of the remaining articles are screened to determine their relevance to secure routing protocols and current security in Wireless Sensor Networks. During this step, studies that clearly do not match the

inclusion criteria—such as papers unrelated to WSNs or not addressing security aspects—are excluded. This helps narrow down the number of papers for full-text review.

Step 6: Full-Text Assessment

In this step, the full text of the selected articles is thoroughly reviewed to ensure they meet all the criteria defined in the protocol. This involves checking whether the studies focus on security challenges, routing protocols, or mitigation techniques in WSNs. Papers that do not provide

doi: 10.32622/ijrat.133202511

sufficient technical detail, do not focus on WSNs, or fall outside the review scope are excluded, with reasons for exclusion documented to maintain transparency.

C. *Eligibility*

Step 7: Select Studies

After the full-text review, the final list of eligible studies on secure routing protocols and current security in Wireless Sensor Networks is confirmed. Only studies that meet all inclusion criteria are selected, such as focusing on WSN security, discussing routing protocols, and being published between 2019 and 2025. The selection process is documented clearly, often using a PRISMA flow diagram to show how many papers were included or excluded and why as shown in Figure 2.

D. *Synthesis*

Step 10: Data Synthesis and Analysis

In this step, the extracted data from the selected studies on secure routing protocols and WSN security are organized and analyzed. The studies are grouped based on key themes such as types of attacks, routing protocols used, or mitigation techniques. A comparative analysis is conducted to identify patterns, trends, and differences in how various protocols address specific security threats in WSNs.

Step 11: Assess Certainty of Evidence

Here, the overall quality and strength of the evidence from the reviewed studies are evaluated. Factors like the clarity of results, consistency across studies, and how well the studies were conducted are considered. This helps determine how reliable the conclusions are and whether they can be confidently used to guide future research or practical implementation.

Step 12: Report Results

Finally, the review findings are presented, following the structure of the PRISMA guidelines. This includes summaries of the types of attacks found in WSNs, the secure routing protocols identified, their advantages and limitations, and potential areas of application. The results also highlight gaps in the current research and suggest directions for future studies in WSN security.

1. Reporting and Interpretation

This section examines the answers to the research questions identified in the analyzed papers. The study examines attacks in wireless sensor networks (WSNs) and the strategies employed to counteract these threats, as well as the current secure routing protocols, highlighting their benefits, drawbacks, and applicable domains. It also explores technologies and methodologies that could shape the future development of secure routing protocols in WSNs. The research results are organized in accordance with the study questions:

RQ 1: What are the main attacks in WSNs and the strategies used to mitigate these attacks?

Wireless Sensor Networks (WSNs) are vulnerable to various security attacks due to their resource-constrained nature, open wireless communication, and often unattended deployment [19]. These attacks can be broadly categorized into routing attacks, data integrity attacks, and physical layer attacks. Each type of attack targets different aspects of the network, and researchers have developed numerous mitigation strategies to address them [20], Some of the main attaches identified include [20], [21], [22], and [23] :

Sybil attacks which pose a significant threat to Wireless Sensor Networks by allowing a single malicious node to present multiple fake identities to other nodes in the network [24]. This undermines the integrity of routing, voting, data aggregation, and resource allocation processes, as the attacker can appear to be multiple nodes at once. Such manipulation can lead to false routing paths, increased resource usage, and disruption of consensus-based protocols. To mitigate Sybil attacks, various strategies have been proposed. One common approach is identity verification using cryptographic authentication, where nodes are required to present valid credentials that are difficult to forge. Trust and reputation systems can also detect abnormal behavior by monitoring node interactions over time and isolating suspicious identities. Additionally, radio resource testing which checks whether claimed identities can transmit on multiple channels simultaneously helps identify fake nodes, as a single device typically cannot handle concurrent transmissions. These mitigation techniques, when combined, enhance the resilience of WSNs against Sybil attacks while maintaining lightweight operation suitable for resource-constrained environments [25].

Another attack in WSNs is Sinkhole attacks. They are a critical security threat in Wireless Sensor Networks, where a compromised node falsely advertises an optimal path to the base station, attracting a significant portion of the network traffic [26];. Once the traffic is rerouted through this malicious node, it can selectively drop, alter, or misroute packets, thereby disrupting data delivery

doi: 10.32622/ijrat.133202511

and compromising the integrity of the network. This type of attack exploits the trust-based and energy-efficient nature of WSN routing protocols. To mitigate sinkhole attacks, geographic routing protocols can be employed, which use physical location data to make routing decisions, thereby reducing the reliance on potentially false route metrics. Trust-based systems are also effective, as they evaluate the behavior of nodes over time and isolate those showing signs of malicious activity. Anomaly detection mechanisms that monitor routing patterns for irregular behavior, such as sudden changes in traffic flow or unusually high route requests, can help in the early identification of sinkhole nodes. Additionally, employing multi-path routing ensures that data is sent through multiple routes, minimizing the impact if one path is compromised. Together, these strategies help maintain secure and reliable communication in WSNs, even in the presence of malicious entities [27].

Wormhole attacks are also one of the most challenging threats in Wireless Sensor Networks, where two or more colluding malicious nodes create a low-latency link called a wormhole between distant parts of the network [28]. This tunnel allows them to replay packets and create the illusion that nodes far apart are neighbors, thereby disrupting routing paths and enabling further attacks like sinkhole or selective forwarding. Wormhole attacks are particularly dangerous because they can be launched without compromising any nodes or breaking encryption [29]. To mitigate these attacks, one effective strategy is the use of packet leashes, which involve adding either geographical or temporal constraints to packets to limit their transmission range or time. Geographic leashes use the physical location of nodes to verify the legitimacy of packet paths, while temporal leashes rely on strict time synchronization to ensure packets are received within expected time windows. Another approach is distance-bounding protocols, which measure the time it takes for a message to travel between nodes to estimate distance and detect anomalies. Localization-based techniques and multi-path routing also help by verifying the plausibility of routing paths and reducing reliance on any single node or link. These combined strategies strengthen WSNs against wormhole attacks while considering their inherent resource constraints. [29]

Hello flood attacks are a type of network-layer threat in Wireless Sensor Networks where an attacker sends or replays HELLO packets with high transmission power to convince many nodes that it is their neighbor. As a result, affected nodes may attempt to route data through the attacker, leading to dropped messages or disrupted communication. This attack exploits the trust that nodes place in HELLO messages used for neighbor discovery and routing table setup [30]. To mitigate hello flood attacks, bi-directional link verification is essential nodes should only accept another node as a neighbor if it can both receive and respond to its messages. Signal strength assessment and location verification can also help detect inconsistencies in transmission power or node proximity. Additionally, implementing authentication mechanisms ensures that only trusted nodes can participate in the routing setup. Some protocols also introduce time-based or cryptographic checks to validate the legitimacy of HELLO packets. These strategies collectively help reduce the effectiveness of hello flood attacks while preserving the lightweight operation necessary for resource-constrained WSN environments [31].

Selective forwarding, also known as Greyhole attacks, is a subtle and harmful security threat in Wireless Sensor Networks where a compromised node selectively drops some packets while forwarding others [32]. Unlike blackhole attacks, where all packets are discarded, greyhole attacks are harder to detect because the malicious node appears to behave normally most of the time. This attack can disrupt data delivery and compromise the reliability and integrity of the network, especially in applications requiring consistent and complete data transmission. According to [33], [34] to mitigate selective forwarding attacks, watchdog mechanisms are commonly used, where nodes monitor their neighbors', packet forwarding behavior and report any discrepancies. Multi-path routing is another effective strategy, ensuring data is sent through multiple redundant paths, making it less likely that all copies of a message will be dropped. Trust and reputation systems can also help by evaluating node behavior over time and isolating nodes with suspicious activity. Additionally, acknowledgment-based protocols and secure routing schemes that verify end-to-end delivery can enhance detection and resilience against such attacks. These combined methods help maintain robust communication even in the presence of selective forwarding threats.

Replay attacks in Wireless Sensor Networks occur when an adversary intercepts legitimate messages and retransmits them at a later time to confuse or disrupt normal network operations [32].

doi: 10.32622/ijrat.133202511

This can lead to outdated or incorrect information being processed, duplication of data, or manipulation of routing paths. Since WSNs often use simple protocols and have limited memory and processing capabilities, they can be particularly vulnerable to this type of attack. To mitigate replay attacks, data freshness mechanisms such as timestamps, sequence numbers, or nonces are commonly employed [35]. These techniques ensure that each packet is unique or recent, allowing the receiving node to recognize and discard replayed messages. Additionally, integrating lightweight cryptographic techniques that include freshness checks can help prevent attackers from injecting previously captured data into the network. Periodic key updates and session-based communications also reduce the window of opportunity for successful replays. These strategies enhance the network's resilience without placing excessive demands on sensor node resources.

Node capture attacks represent a severe physical threat to Wireless Sensor Networks, where an attacker physically seizes a sensor node to extract sensitive data such as cryptographic keys, routing information, or stored messages [32] . Since WSNs are often deployed in open or hostile environments, they are particularly susceptible to this type of attack. Once compromised, the attacker can clone the node, inject false data, or use the obtained credentials to launch further attacks like Sybil or sinkhole attacks [36]. To mitigate node capture attacks, deploying tamper-resistant hardware can make it more difficult or costly for attackers to access internal data. Dynamic key management schemes, where keys are updated regularly or generated per session, can limit the usefulness of any extracted information. Additionally, intrusion detection systems and trust-based frameworks can monitor for unusual behavior that might indicate a compromised node. Another strategy is to design the network with limited node knowledge, so each sensor is only aware of a small portion of the network, reducing the damage if it is captured. These countermeasures collectively improve the overall security and robustness of WSNs against physical compromise [37].

TABLE 2: COMPARATIVE TABLE OF WSN ATTACKS AND MITIGATION TECHNIQUES

Attack Type	Impact on WSN	Mitigation Strategies	Effectiveness
Sybil Attack	Identity spoofing, routing disruption	Identity verification, trust management	Moderate (depends on trust level)
Sinkhole Attack	Traffic misrouting, data loss	Geographic routing, anomaly detection, trust models	High (with trust + monitoring)
Wormhole Attack	False route formation, network confusion	Packet leashes, distance bounding, multi-path routing	High (but costly in resources)
Hello Flood Attack	False neighbor discovery	Signal strength verification, bi-directional check	Moderate
Selective Forwarding Attack	Partial data loss, undetected misbehavior	Watchdog, multi-path routing, reputation systems	High (with cooperative detection)
Replay Attack	False route/data re-injection	Nonce, timestamp, freshness checking	High
Node Capture Attack	Compromised node, key leakage	Tamper-resistant nodes, key renewal	Low to moderate (costly)

RQ 2: What secure routing protocols have been developed for Wireless Sensor Networks, and their respective strengths, weaknesses, and areas of application?

Wireless Sensor Networks (WSNs) require secure routing protocols to ensure data confidentiality, integrity, and availability in the face of various attacks. Over the years, numerous secure routing protocols have been proposed, each designed with specific security goals and network constraints in mind. Below is a discussion of some widely studied secure routing protocols, highlighting their strengths, limitations, and typical application domains [38], [39], [40] and [41].

doi: 10.32622/ijrat.133202511

TABLE 3: COMPARATIVE TABLE OF SECURE ROUTING PROTOCOLS IN WSNS

#	Protocol / Focus	Security Features	Strengths	Weaknesses	Applications
1	SEARP – Secure Energy Aware Routing Protocol [38]	- EdDSA-based node authentication - Wormhole attack prevention - Secure cluster head communication	- Strong cryptographic authentication - Wormhole resistance - Energy-efficient	- Public-key cryptography overhead - Signature verification delays	Military & industrial WSNs requiring high-level security
2	Trust-GA Routing – Trust-based with Adaptive Genetic Algorithm [41]	- Trust evaluation to avoid malicious nodes - Secure route discovery and maintenance	- Dynamic route optimization - Good trade-off between energy & trust	- High computation for constrained nodes - Requires trust initialization	IoT-based sensor networks in dynamic, hostile environments
3	ITEERP – Improved Trust-based Energy Efficient Routing Protocol [40]	- Node and path trust monitoring - Reputation management - Detection of misbehaving nodes	- Prolonged network lifetime - Efficient detection of compromised nodes	- Overhead from regular trust updates - Risk of trust poisoning	Urban environmental WSNs, smart agriculture, community IoT
4	Multi-tier Trust Routing [42]	- Trust management framework - Link quality estimation - Blacklisting of malicious nodes	- Scalable trust model - Robust against insider threats	- Design complexity - Sink node bottleneck	Large-scale IoT applications, smart cities
5	Energy-Efficient Trust Protocol using GA , [39]	- Trust scoring - Blackhole and selective forwarding prevention - Secure path selection	- Adaptive, trust-driven routing - Secure data delivery	- Computational load from genetic algorithm - Learning curve for trust values	WSNs in resource-constrained, attack-prone deployments
6	ESR Energy-Efficient Secure Routing with Secret Sharing [43]	Secret sharing, encrypted cluster communication	Secure, energy-efficient, intrusion tolerant	Communication/key-sharing overhead	Large-scale IoT WSNs
7	SeRINS Secure Routing in Sensor Networks [43]	Neighbor-based route verification, isolation of compromised nodes	Selective-forwarding resilience	No encryption; colluding vulnerability	Cooperative, cluster WSNs
8	IASR Information-Aware Secure Routing [44]	Trust thresholds, forwarding classification, isolation	Delivers under high malicious load	Tuning thresholds, logic overhead	Hostile/deception-prone environments

RQ 3: What strategies may influence the future design of secure routing protocols in WSNs?

From the study the future design of secure routing protocols in Wireless Sensor Networks (WSNs) is expected to be shaped by several evolving strategies and technologies that address both security challenges and the limitations of sensor nodes. As WSN applications grow in complexity—from smart agriculture to critical infrastructure—the need for robust, scalable, and energy-efficient secure routing becomes even more pressing. The study identified the following strategies which are likely to influence future protocol design [45], [46], [47], [48], [49], [50]

1. Integration of Lightweight Cryptography

Future secure routing protocols will increasingly rely on lightweight cryptographic algorithms tailored for resource-constrained environments. These cryptosystems offer strong encryption and authentication with minimal computational and energy overhead. Lightweight block ciphers like PRESENT and LEA are expected to become standard components in routing protocols to secure data transmission without draining battery life [51].

2. Trust and Reputation-Based Systems

As insider threats and node compromise become more prevalent, trust-based routing will play a vital role. These systems dynamically assess the behavior of nodes based on past interactions to evaluate trustworthiness. Trust models help in isolating malicious nodes and promoting reliable ones, thereby increasing network resilience [52].

3. Machine Learning and Anomaly Detection

doi: 10.32622/ijrat.133202511

Machine learning (ML) techniques are being explored to detect abnormal routing behavior in WSNs. Protocols that incorporate ML models can analyze traffic patterns and node behaviors to identify and respond to threats like selective forwarding or Sybil attacks in real time. These intelligent protocols will adapt to new types of attacks that may not be detectable by static rules [53].

4. Blockchain and Distributed Ledger Technologies (DLTs)

The decentralization and immutability of blockchain technology can be leveraged to enhance trust and data integrity in WSNs. Future secure routing protocols may use lightweight blockchain systems to maintain secure routing information and authenticate node identities in a distributed and tamper-proof manner, thereby reducing the impact of single points of failure [48].

5. Cross-Layer Security Approaches

Next-generation routing protocols will adopt cross-layer security strategies that combine information from multiple layers of the protocol stack (e.g., MAC, network, application layers). This approach allows for more comprehensive threat detection and mitigation, such as correlating energy anomalies at the physical layer with routing misbehavior at the network layer [49].

6. Energy-Aware Security Mechanisms

As energy efficiency remains a top priority, future protocols will optimize the trade-off between security and energy consumption. Techniques like adaptive security levels—where higher security is applied only when a threat is detected—will help prolong network life while maintaining robust protection [50].

7. Mobility and Dynamic Topology Support

With the increasing use of WSNs in applications involving mobility (e.g., healthcare, military), secure routing protocols will need to be adaptive to frequent topology changes. Protocols must ensure secure path discovery and maintenance even in rapidly changing environments, possibly using predictive routing mechanisms and mobility-aware trust evaluation [54].

8. Quantum-Resistant Algorithms

Though still in early research stages, quantum-resistant cryptographic methods may become essential for future WSN security. These algorithms are designed to resist attacks from quantum computers, providing long-term data protection in mission-critical sensor networks [55].

IV. Discussion

The study intends to evaluate current research on secure routing methods in wireless sensor networks. PRISMA systematic literature technique and suggestions were employed in the study (2020. Data were collected from original studies published in journal articles, conference proceedings, and selected preprints between 2019 and 2025. After applying our selection criteria, the study found 100 suitable publications. The study's discussions are summarized as follows:

RQ1. The first research question was to identify the main attacks in WSNs and the strategies used to mitigate these attacks. The research revealed that there are numerous types of attacks in wireless sensor networks. Some of the common attacks include Sybil attacks, where a node illegitimately claims multiple identities to disrupt routing; sinkhole attacks, where a compromised node attracts traffic to drop or alter packets; wormhole attacks, which create a shortcut in the network to mislead routing decisions; and selective forwarding (grey hole) attacks, where nodes drop packets selectively to avoid detection. Other notable threats include hello flood, replay, and node capture attacks. Also, the study found that various strategies have been developed to mitigate these attacks. These strategies include Authentication and encryption, Trust and reputation systems, Geographic and temporal packet leashes, redundant routing paths and intrusion detection systems, and Tamper-resistant hardware and secure key management as seen in Table 2 above.

RQ2. The study's second objective was aimed at identifying secure routing protocols that have been developed for Wireless Sensor Networks, and what are their respective strengths, weaknesses, and areas of application. From the study the research revealed that numerous types of secure routing protocols in wireless sensor networks have been developed over the years. Some of the identified secure routing protocols are SEARP, ITEERP, ESR, SeRINS, and IASR but they still have some limitations as seen in Table 3. Each protocol addresses specific threats and network configurations, and their adoption depends on factors such as energy constraints, network scale, mobility, and required security level.

RQ3. The study's third goal was accessing the strategies may influence the future design of secure routing protocols in WSNs. The research identified Several emerging strategies that are expected to shape the design of future secure protocols for WSNs. These strategies included lightweight cryptography, trust-based and reputation systems, machine learning and anomaly detection, blockchain and distributed ledger technologies, Cross-Layer Security Approaches, Energy-Aware Security Mechanisms, Mobility and Dynamic Topology Support, and Quantum-Resistant Algorithms. These strategies are aimed at developing secure routing protocols that are resilient, adaptive, and sustainable, making WSNs more reliable and secure in complex and hostile environments.

V. Conclusion and Future Works

This review has explored the current trends and developments in secure routing protocols for Wireless Sensor Networks (WSNs). Many protocols have been proposed to protect against threats such as blackhole, wormhole, Sybil, and selective forwarding attacks. These solutions use different techniques like cryptography, trust management, and hybrid approaches. While they improve security, each has its own limitations in terms of energy use, scalability, and adaptability to changing environments.

doi: 10.32622/ijrat.133202511

Recent trends show that researchers are moving toward lightweight, energy-efficient, and intelligent protocols that can adapt to dynamic network conditions. New technologies such as machine learning, blockchain, and post-quantum cryptography are beginning to shape the future of secure routing in WSNs. These technologies offer potential for stronger, more adaptive, and more autonomous routing decisions in real-world applications.

In future work, researchers should focus on developing protocols that are resistant to future quantum attacks, can adapt to node mobility and topology changes, and support real-time decision-making using AI. There is also a need for standardized test environments to evaluate protocol performance and security under common benchmarks. This will help guide the development of practical, secure, and efficient routing solutions for next-generation WSNs.

REFERENCES

[1] P. Chaudhary and A. Waoo, "Wireless Sensor Network For Environmental Monitoring," International Research Journal of Modernization in Engineering Technology and Science, vol. 5, no. 11, pp. 604-607, 2024.

[2] K. Anand, S. Tanuj and K. Amit, "Blockchain technology for smart wireless sensor networks," Elsevier, pp. 251-270, 2025.

[3] K. D, N. C, V. D and K. G., " Applications of wireless sensor networks: An up-to-date survey.," Appl. Syst. Innov. , vol. 3, no. 14, 2020.

[4] S. Ambareesh, P. Chavan, S. Supreeth and e. al., "A secure and energy-efficient routing using coupled ensemble selection approach and optimal type-2 fuzzy logic in WSN.," Sci Rep, vol. 15, no. 38 , 2025.

[5] M. A. Khan and M. Imran, "Secure routing in wireless sensor networks: Attacks and countermeasures,"," IEEE Access, vol. 8, pp. 1-20, 2020.

[6] S. A. Aljawarneh, " "A systematic review of routing attacks detection in wireless sensor networks,"," Sensors, vol. 20, no. 9, pp. 1-25, 2020.

[7] A. P. Kumar, S. R, C. M, S. Dhananjaya and K. M. N, "An energy-efficient and secure WSN routing protocol using Bayesian networks and elitist genetic algorithms.," Journal Européen des Systèmes Automatisés, vol. 57, no. 6, pp. 1547-1555, 2024.

[8] A. S, J. N, U. S, K. AU, Q. AM and C. JG., " Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks.," Sensors, vol. 22, no. 2, 2022.

[9] A. Sultana, K. u. R. Khan and K. Prasad, "An Overview of Cluster-Based Routing Protocols in Wireless Sensor Networks: A Survey," Journal of Electrical Systems, vol. 9, p. 20, 2024.

[10] A. Alabady, A. Alsarhan and R. Abuarqoub, "Security challenges and solutions in wireless sensor networks: A survey," IEEE Access, vol. 8, p. 219339–219364, 20202.

[11] H. Khaled, M. Mohamed Ashraf and S. Nouh, "A Review of Security Challenges and Solutions in Wireless Sensor Networks," Journal of Al-Azhar University Engineering Sector, vol. 18, no. 69, pp. 914 - 938, 2023.

[12] A. Boudia and M. Feham, "Trust-based routing protocols in WSNs: A survey,," Computers & Security, vol. 85, p. 57–78, 2019.

[13] H. Chen, " Secure routing protocols in wireless sensor networks: A review," Sensors, vol. 20, no. 7, 2020.

[14] M. Javed, "Routing protocols and security issues in wireless sensor networks: A review,," IEEE Access,, vol. 7, p. 97558–97573, 2019.

[15] M. F. e. al, "BTSR: A blockchain-enabled trust-based secure routing protocol for WSNs," Future Generation Computer Systems, vol. 124, p. 411–426, 2021.

[16] A. Gupta and V. Singh, "ML-SRP: A machine learning-based secure routing protocol for WSNs," Computer Networks,, vol. 194, p. 108138, 2021.

[17] T. Susnjak, "PRISMA-DFLLM: An Extension of PRISMA for Systematic Literature Reviews using Domain-specific Finetuned Large Language Models," arXiv preprint arXiv, pp. 1-20, 2023.

[18] E. Elsman, L. Mokkink, C. Terwee and e. al., " Guideline for reporting systematic reviews of outcome measurement instruments (OMIs): PRISMA-COSMIN for OMIs 2024. 8, 64 (2024)," J Patient Rep Outcomes, vol. 6, no. 64, 2024.

[19] K. Dionisis, N. Christos, V. Dimitrios and K. Grigorios, "Applications of wireless sensor networks: An up-to-date survey. Appl. Syst. Innov. 3, 1 (2020), 14," survey. Appl. Syst.Innov, vol. 3, no. 14, 2020.

[20] O. Ahmet, H. Reza, A. Ozkan and K. Oztoprak, "Security Challenges, Mitigation Strategies, and Future Trends in Wireless Sensor Networks: A Review," ACM Computing Surveys, vol. 57, no. 4, pp. 1-29, 2024.

[21] J. Ayuba, F. I. Ismail and H. M. Syed Hamid, "Current Security Threats in Applications of Wireless Sensor Network," International Journal on Engineering, Science, and Technology, vol. 5, no. 3, pp. 255- 272 , 2023.

[22] S. Maahiya and S. W. Kim, "Security in Wireless Sensor Networks Using OMNET++: Literature Review," Sensors , vol. 25, no. 10, p. 2972, 2025.

[23] M. M. Moslehi, "Exploring coverage and security challenges in wireless sensor networks: A survey," Computer Networks, vol. 260, 2025.

[24] A. Reham and A.-S. Eman, " Sybil attack detection scheme based on channel profile and power regulations in wireless sensor networks.," Wireless Network, vol. 28, no. 4, p. 1361–1374., 2022.

[25] A. Arthanareeswaran, T. P. Saravanabava, P. Sakthivel and K. S. Vishvaksenan, " Novel Sybil attack detection using RSSI and neighbour information to ensure secure communication in WSN.," Journalof Ambient Intell. Human. Comput., vol. 12, p. 6567–6578., 2021.

[26] A. Mubashir, N. Muhammad, S. Ayesha, A. Shahbaz and A. Ijaz., "Addressing sinkhole attacks in wireless sensor networks—a review.," International Journal of Scientific & Technology Research, vol. 9, no. 08, p. 406–411, 2020.

[27] P. C. Kala, A. P. Agrawal and R. R. Sharma., "A novel approach for isolation of sinkhole attack in wireless sensor networks.," in In Proceedings of the 10th International Conference on Cloud Computing, Data Science & Engineering(Confluence), 2020.

[28] H. Maria, A. Humaira, Zakia, Jalil, Z. J. Noor, H. Mamoona, S. Saqib and M. A. Abdullah, " AI-based wormhole attack detection techniques in wireless sensor networks.," Electronics, vol. 11, no. 15, p. 2324, 2022.

[29] S. Surinder and S. S. Hardeep, " Intelligent ad-hoc on demand multipath distance vector for wormhole attack in clustered WSN," Wireless Personal Commun., vol. 122, no. 2, p. 1305–1327, 2022.

[30] T. A. S. Srinivas and S.S. Manivannan, "Prevention of Hello Flood Attack in IoT using combination of Deep Learning with Improved Rider Optimization Algorithm," Computer Communications, vol. 163, pp. 162-175, 2020.

[31] A. Zainab, B. A. Nor, K. Amirrudin and B. Mohammad Riyaz, "A systematic review of routing attacks detection in wireless sensor networks," Peer J Comput Sci, 2022.

[32] D. S. M. Keerthika, "Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures,," Global Transitions Proceedings, vol. 2, no. 2, pp. 362-367,, 2021.

[33] S. Surinder and S. S. Hardeep, "Learning-Based Security Technique for Selective Forwarding Attack in Clustered WSN," Wireless Personal Communications, vol. 118, no. 1, pp. 789 - 814, 2021.

[34] O. Ahmet, H. Reza, O. Aysegul and K. Oztoprak, "Security Challenges, Mitigation Strategies, and Future Trends in Wireless Sensor Networks: A Review," ACM Computing Surveys, vol. 57, no. 4, pp. 1 - 29, 2024.

[35] R. Pichamuthu, S. A and K. N, "An Enhanced Deep Learning Approach for Preventing Replay Attacks in Wireless Sensor Network," Solid State Technology, vol. 63, no. 4, pp. 1-14, 2020.

[36] W. Chenyu, W. Ding, T. Yi, X. Guoai and W. Huaxiong, "Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks," IEEE Transactions on Dependable and Secure Computing, vol. 19, pp. 507-523, 2022.

[37] L. Jing, L. Lihui, L. Zenghui, L. Yingxu, Q. Hua and L. Shiyao, "WSN node access authentication protocol based on trusted computing,"

doi: 10.32622/ijrat.133202511

Simulation Modelling Practice and Theory, vol. 117, 2022.

[38] A. Alateeq, W. Elmedany, N. Ababneh and K. Curran, "Secure energy aware routing protocol for IEEE 802.15.4 wireless sensor networks," Journal of Engineering, Design and Technology, vol. 20, no. 3, p. 569–594, 2022.

[39] Y. Han, H. Hu and Y. Guo, "Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm," IEEE Access, vol. 10, pp. 11538-11550, 2022.

[40] J. B. S. Loret and T. G. Kumar, "An Improved Trust Based Energy Efficient Routing Protocol for Wireless Sensor Networks," Journal of Internet Technology , vol. 22, no. 7, pp. 1509-1515, 2021.

[41] H. Huangshui, H. Youjia, Y. Meiqin and X. Song, "Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks," IEEE Access, vol. 10, pp. 10585-10596, 2022.

[42] H. Huangshui, H. Youjia, Y. Meiqin and S. Xue, "Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks," IEEE Access, 2021.

[43] H. Khalid, A. Ahmad, A. Ahmad, A. Ahmad and Z. Jan, "An Energy-Efficient and Secure Routing Protocol for Intrusion Avoidance in IoT-Based WSN," Energies , vol. 12, no. 21, pp. 1-18, 2019.

[44] Q. Shi, L. Qin, Y. Ding, B. X. J. Zheng and L. Song, "Information-Aware Secure Routing in Wireless Sensor Networks," Sensors, vol. 20, no. 165, pp. 1-21, 2019.

[45] V. A. Thakor, M. A. Razzaque and M. R. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," IEEE Access, vol. 9, pp. 28177-28193, 2021.

[46] S. Alaa, J. Pallavi, J. Pallavi and S. S. Sengar, "Trust-Aware Routing Mechanism through an Edge Node for IoT-Enabled Sensor Networks," Sensors, vol. 22, no. 20, 2022,.

[47] M. S. B. e. al, "AI-Based Decision Support System Optimizing Wireless Sensor Networks for Consumer Electronics in E-Commerce," Applied Science, vol. 14, pp. 2-24, 2024.

[48] Y. Liu et al., "Blockchain and Deep Learning Based Secure Routing for IoT-WSNs," Computers, Materials and Continua(CMC), vol. 7, no. 3, p. 435–458, 2024.

[49] K. Zhao and L. Ge, ""Cross-layer Design for Security in WSNs," IEEE Commun. Surv., vol. 23, no. 2, p. 1265–1286, 2021.

[50] A. Khan and e. al, "Energy Efficient Secure Routing in WSNs: Survey and Open Issues," EEE Access, vol. 8, p. 156832–156856, 2020.

[51] I. Radhakrishnan, S. Jadon and P. B. Honnavalli, "Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices," Sensors, vol. 24, no. 12, pp. 1-19, 2024.

[52] Z. Yang, L. Li, F. Gu, X. Ling and Maryam Hajiee, "TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks," Internet of Things, vol. 20, p. 100627, 2022.

[53] R. Priyadarshi, R. Kumar, R. R. R. and e. al, "AI-based routing algorithms improve energy efficiency, latency, and data reliability in wireless sensor networks," Sci Rep, vol. 15, 2025.

[54] M. Al-Fuqaha and e. al, "SDN-Based Mobility-Aware Secure Routing for Smart Cities," EEE Commun. Mag, vol. 59, pp. 44-50, 2021.

[55] H. Hölzl and H. Lipmaa, "Lightweight Post-Quantum Authentication for the Internet of Things," IEEE Access, vol. 9, p. 21943–21958, 2021.

AUTHORS PROFILE

Peter Maina Mwangi is a Lecturer in the Department of Computing and Information Technology Mama Ngina University College, Kenya. He received his BSc. in Computer Science from Busoga University, Uganda in 2010, his MSc in Data Communication and Networks from KCA University, Kenya in 2018 and PhD in Computer Science from Murang'a University of Technology, Kenya in 2024. His Research interest is in Computer Network, Security, artificial Intelligence. He is a Professional Member of Institute of Electrical and Electronics Engineers (IEEE), the International Association of Engineers (IAENG) and Scientific & Technical Research Association (STRA)

[1] **Juliet Gathoni Muchori** received his B.Sc. in Information Technology (2017) from Muranga University of Technology in Kenya. An M.Sc. in Information Technology (2021) from Murang'a University of Technology, Kenya. Currently, he is pursuing Ph.D. Information Technology and serving as a Technologist in the department of Information Technology, Murang'a University of Technology. Her research interests include Internet of things, Machine Learning and Natural Language Processing.

doi: 10.32622/ijrat.133202511