Secure Routing Protocols for Wireless Sensor Networks: Design, Analysis, and Novel Framework Proposal

Deepika Komal
Assistant Professor, Department of Computer Science, Dashmesh Khalsa College, Zirakpur

***Abstract*— Wireless Sensor Networks (WSNs) have emerged as a foundational technology in modern communication and monitoring systems, enabling widespread applications in environmental surveillance, military operations, healthcare monitoring, industrial automation, and smart cities. Despite their advantages in scalability and self-organised operation, WSNs are highly vulnerable to routing-based attacks due to their resource limitations, dynamic topology, and unreliable communication medium. Ensuring secure routing remains a critical research challenge, requiring lightweight yet robust solutions capable of resisting malicious intrusions while optimising energy consumption.**

This paper presents a comprehensive review of secure routing protocols for WSNs, analyses their strengths and limitations, and identifies persistent research gaps. Further, we propose a Novel Hybrid Lightweight Secure Routing Framework (HLSRF) based on trust evaluation, dynamic key generation, and anomaly-aware routing decision mechanisms suited for constrained sensor nodes. A simulation-driven performance study demonstrates improvements in packet delivery ratio, resilience against selective forwarding, and reduced energy consumption compared to existing schemes. The findings establish HLSRF as a promising approach for future secure WSN deployments.

***Index Terms*— Wireless Sensor Networks, Secure Routing, Cryptographic Mechanisms, Trust Management, Energy Efficiency, Intrusion Detection, Lightweight Security**

I. INTRODUCTION

Wireless Sensor Networks consist of spatially distributed sensor nodes capable of sensing, processing, and transmitting environmental data to a central sink or base station. Their low cost and deployment flexibility have made WSNs integral to critical infrastructures, including smart agriculture, disaster management, habitat monitoring, battlefield tracking, and health surveillance systems. However, the broadcast-based communication nature and absence of centralised control make WSNs prone to serious security threats such as eavesdropping, spoofing, selective forwarding, sinkhole, Sybil, and wormhole attacks.

Routing protocols in WSNs primarily focus on reducing energy consumption to extend network lifetime. Security, although equally important, often remains secondary due to computational and memory limitations of nodes. Traditional security approaches used in MANETs and IoT systems are not directly adoptable in WSNs. Consequently, designing energy-efficient secure routing strategies has become an active research domain.

This study presents:

1. An overview of WSN architecture and routing challenges
2. Classification of routing protocols with focus on secure routing
3. Analysis of cryptographic, trust-based, and intrusion-detection routing mechanisms
4. Identification of major open research issues
5. Proposal of a Novel Hybrid Lightweight Secure Routing Framework (HLSRF)

The aim is to contribute a scalable and secure routing approach tailored for constrained resource microcontrollers commonly used in sensor nodes.

II. WIRELESS SENSOR NETWORKS

Wireless Sensor Networks represent a distributed collection of miniature sensor nodes deployed across a physical or geographical environment to monitor parameters such as temperature, pressure, vibration, pollution, and motion. These nodes collaborate to form an intelligent sensing ecosystem where data is

periodically or event-wise forwarded to a central sink or base station for further processing and decision-making. Due to their low cost, mobility, and autonomous operation, WSNs have become a core enabling technology for next-generation applications including smart agriculture, smart homes, industrial automation, environmental conservation, battlefield surveillance, and medical telemetry.

A typical sensor node comprises four fundamental components:

- Sensing Unit: equipped with analog-to-digital converters to capture environmental stimuli.
- Processing Unit: usually a microcontroller or microprocessor responsible for data computation, routing decisions, and protocol execution.
- Radio Transceiver: handles wireless communication between nodes, enabling multi-hop networking.
- Power Unit: a compact battery supply, often non-rechargeable, making energy preservation crucial for prolonged network operation.

The collective behaviour of these nodes enables a self-configuring and self-healing wireless network capable of operating in harsh and unattended environments.

2.1 Network Architecture

The architectural model adopted in a WSN significantly influences routing, energy distribution, and scalability. Broadly, WSNs follow three commonly recognised structural designs:

1. Flat (Distributed) Architecture: In this architecture, every sensor node holds equal responsibilities in sensing and forwarding data. Routing decisions are made collaboratively without hierarchical control, enabling simplicity and robustness. Flat architectures are effective for small to medium-sized deployments; however, as network scale increases, routing overhead and energy consumption may rise.
2. Hierarchical (Cluster-Based) Architecture: Nodes are organized into clusters, and a designated Cluster Head (CH) manages intra-cluster communication, aggregation, and forwarding of aggregated data to the base station. This structure reduces communication load and improves energy efficiency. Many energy-aware routing protocols like LEACH are based on this architecture due to its balanced load distribution.
3. Location-Based Architecture: Routing decisions are influenced by geographical information such as GPS coordinates or estimated node location using localization algorithms. Data packets are forwarded based on distance metrics, making this method suitable for large spatial deployments where distance-aware routing reduces redundant transmissions.

2.2 Communication Model

Data flow patterns in WSNs determine how sensed information travels from ordinary nodes to the sink. The most prevalent communication models include:

- Direct Communication: Nodes transmit sensed data directly to the sink without intermediate hops. While simple, it is energy-expensive for distant nodes, leading to rapid battery depletion.
- Multi-Hop Routing: Data is forwarded through several intermediate nodes before reaching the base station. This strategy balances energy consumption and extends network lifetime, especially in large networks.
- Cluster-Based Routing and Aggregation: Nodes forward data to their respective cluster heads, where aggregated data is compressed and transmitted further. This reduces transmission redundancy, bandwidth consumption, and overall network load.

2.3 Design Requirements

The performance of a WSN depends on efficient protocol design. A secure routing protocol must satisfy the following criteria:

- Low Energy Consumption: Since nodes have limited power sources, communication must be optimised to reduce unnecessary transmissions and prolong network lifetime.
- Scalability:
  The routing mechanism should support thousands of nodes without causing congestion or excessive control overhead.
- Data Security and Confidentiality: Information must remain protected from unauthorised access, especially in military, health, and industrial surveillance environments.

- Fault Tolerance and Self-Recovery: The network should maintain operational continuity even if nodes malfunction, deplete energy, or are physically damaged.
- Computational Efficiency: Lightweight algorithms are essential to avoid memory and processing overload in resource-constrained sensor motes.

These design considerations form the foundation for developing robust and resilient routing strategies.

Attack Type	Brief Description	Impact on the Network
Sinkhole Attack	A malicious node falsely advertises itself as the most efficient route to attract large volumes of network traffic.	Severe data interception, false routing decisions, data manipulation.
Sybil Attack	A single node assumes multiple fake identities to influence routing tables and resource allocation.	Network confusion, inaccurate routing topology and compromised authentication.
Wormhole Attack	Attackers create a low-latency tunnel between two points in the network, misleading routing decisions.	Artificial shortcut routes, topological distortion, faster network compromise.
Selective Forwarding Attack	Malicious nodes forward only selective packets while dropping others.	Reduced packet delivery ratio, degraded QoS, incomplete monitoring data.
Hello Flood Attack	An adversary transmits powerful HELLO packets to impersonate a neighbor node.	Rapid energy depletion, topology instability, network congestion.
Replay Attack	Previously captured packets were resent or replayed into the network.	Routing confusion, false triggers, unauthorized packet reuse.

2.4 Security Challenges

WSNs differ from traditional wired or MANET infrastructures due to their constrained resources and unattended operation, making them more susceptible to attacks. Critical challenges include:

- Limited Hardware Resources: Sensor nodes possess minimal memory, low CPU power, and restricted bandwidth, limiting the feasibility of heavy cryptographic operations.
- Finite Battery Power: Replacing or recharging batteries is often impractical, particularly in remote or hazardous terrains; therefore, routing security must remain lightweight to conserve energy
- Physical Vulnerability: Nodes can be easily captured or tampered with, enabling attackers to extract keys, alter firmware, or inject false data
- Unreliable Wireless Medium: Environmental noise, interference, and multi-path fading degrade link quality, increasing packet loss and making secure transmission more complex.

Due to these constraints, routing security becomes a critical research priority, requiring innovative solutions that blend authentication, trust evaluation, intrusion detection, and energy-aware routing techniques.

III. DUE TO THE OPEN WIRELESS MEDIUM

distributed nature, and lack of centralised supervision, routing in Wireless Sensor Networks is highly vulnerable to adversarial manipulation. Attackers often exploit multi-hop communication and routing behaviour to disrupt normal data flow, drain node resources, or gain unauthorized access to sensitive information. To ensure secure packet transmission, routing protocols must be resilient against both external intruders and compromised internal nodes.

Several prominent routing attacks typically encountered in WSNs are described below:

Collectively, these attacks target the core security goals of WSNs confidentiality, integrity, availability, and authentication. Therefore, designing routing protocols that can identify, mitigate, and withstand these attacks without imposing heavy computational overhead is a fundamental research priority.

IV. CLASSIFICATION OF SECURE ROUTING PROTOCOLS

To counter security threats in WSNs, researchers have proposed a wide variety of secure routing mechanisms. These techniques can be broadly classified into four primary categories, each differing in methodology, defensive capability, and resource requirements.

4.1 Cryptography-Based Secure Routing Protocols

Cryptographic solutions offer fundamental security services such as authentication, confidentiality, and message integrity. Techniques employed may include symmetric key encryption, asymmetric cryptosystems, hash functions, and Message Authentication Codes (MACs). Popular examples include SPINS (SNEP and μTESLA), TinySec, and TinyPK, which are specifically designed for low-power sensor networks.

Strengths:

- Ensures strong protection against eavesdropping and unauthorised access
- Prevents packet forgery and tampering through encrypted communication

Limitations:

- High computation and memory demand for cryptographic operations
- Key generation, distribution, and revocation increase protocol complexity

Although cryptography forms the first layer of security, relying solely on encryption is insufficient to detect compromised insider nodes, which motivates the use of complementary trust-based strategies.

4.2 Trust and Reputation-Based Routing Protocols

Trust-based protocols evaluate the reliability of nodes using behavioural metrics such as packet forwarding ratio, response consistency, delay tolerance, and cooperation level. Nodes exhibiting suspicious behaviour receive lower trust values and may be isolated from routing paths. Examples of this category include TARP, ATSR, and TMSR.

Advantages:

- Effective in identifying malicious insider nodes
- Enhances reliability and packet delivery in collaborative environments

Challenges:

- Requires continuous monitoring and trust table maintenance
- Trust establishment is slow in newly deployed or mobile networks

Trust-based systems strengthen resilience but introduce overhead when maintaining trust metrics in dense networks.

4.3 Intrusion Detection-Based Secure Routing

Intrusion Detection Systems (IDS) analyse traffic patterns to detect anomalies, attack signatures, or malicious activities during routing. IDS may be signature-based, anomaly-based, or hybrid, with examples including IDSX, SVELTE for 6LoWPAN, and machine-learning-enhanced IDS frameworks.

Benefits:

- Capable of identifying complex and evolving attack behaviours
- Can detect zero-day anomalies beyond traditional encryption scope

Drawbacks:

- Often computationally intensive for resource-constrained sensor motes
- High memory demand for training data and detection models

IDS-based routing can provide proactive protection, but optimising its lightweight deployment in constrained environments remains a challenge.

4.4 Energy-Aware Secure Routing Protocols

Given that WSN nodes operate on limited power, routing strategies must ensure energy-efficient data transmission while still maintaining acceptable security levels. Energy-aware secure protocols integrate authentication mechanisms with load-balanced routing. Techniques include secure variants of LEACH, SEER, and SHEER.

Key Benefits:

- Prolongs network lifetime through optimized cluster-based routing
- Reduces redundant transmissions and enhances sustainability

Trade-Offs:

- Stronger security mechanisms may consume additional computation cycles
- Balancing energy efficiency with high-level security requires design optimization

Thus, energy-aware security is essential for long-term monitoring systems such as ecological observation or remote battlefield networks.

V. EXISTING SECURE ROUTING PROTOCOLS – COMPARATIVE STUDY

Protocol	Technique Used	Key Strength	Limitation
SPINS	Symmetric crypto	Lightweight design	Lacks protection against DoS
TinySec	Link-layer security	Efficient AES-based encryption	No node-level trust
S-MAC	Sleep scheduling	Energy saving	Weak attack resilience
SEER	Key management & trust	Good PDR performance	Storage overhead
RLEACH	Randomized clusters	Better CH rotation	Susceptible to Sybil
SVELTE	IDS for IoT	Strong anomaly detection	High memory requirement

Existing solutions either emphasize cryptography or trust, but few combine them in an optimized lightweight manner.

VI. RESEARCH GAP IDENTIFICATION

From literature analysis:

1. Cryptographic solutions alone are insufficient
   - Not effective against insider attacks
   - Overhead increases energy consumption
2. Trust-based approaches require time to stabilize
   - New nodes have insufficient trust history
3. Lack of hybrid lightweight routing security
   - Need combined cryptographic + trust + anomaly awareness
4. Few protocols self-adapt to dynamic topology changes
   - Especially under high mobility or node failure
5. Energy and security trade-off unresolved
   - A secure protocol must not degrade network lifetime

These gaps motivate a novel integrated framework.

VII. PROPOSED HYBRID LIGHTWEIGHT SECURE ROUTING FRAMEWORK (HLSRF)

7.1 Core Objectives

- Ensure secure, authenticated route establishment
- Detect and isolate malicious nodes dynamically
- Reduce energy consumption through efficient cluster routing
- Provide scalable security with minimal computation overhead

7.2 Architecture Overview

HLSRF integrates:

1. Lightweight Symmetric Key Encryption (LSE)
   - Keys generated per session using hash chaining
2. Trust Evaluation Engine (TEE)
   - Trust score composed from forwarding behaviour, latency, packet drop ratio
3. Anomaly Detection Unit (ADU)
   - Identifies abnormal traffic patterns using threshold deviation
4. Energy-aware Cluster Routing (ECR)
   - Cluster head chosen based on residual energy + trust score

Routing Decision Formula:

[RouteScore = \alpha T_r + \beta E_r + \gamma S_r]

Where:

- (T_r) = trust value
- (E_r) = remaining energy
- (S_r) = security level from anomaly unit
- α, β, γ are weighted coefficients adjustable by scenario

7.3 Key Generation Algorithm (Simplified)

Step 1: Base station generates initial key K0

Step 2: For each round i:

Ki = hash(K(i-1) || nodeID || timestamp)

Step 3: Keys expire automatically after period t

Step 4: Compromised node revocation via broadcast hint

This dynamic mechanism prevents replay and key reuse attacks.

7.4 Trust Computation Model

Trust value Ti calculated from:

[T_i=\frac{W_fF_i + W_dD_i + W_lL_i}{W_f+W_d+W_l}]

Where:

- (F_i) = forwarding ratio
- (D_i) = drop count
- (L_i) = delay factor
- Wi = weight parameters

Nodes below trust threshold τ are blacklisted.

7.5 Working of Proposed Routing

1. Nodes form clusters through energy-trust score selection
2. CH broadcasts encrypted session key using LSE
3. Data packets monitored for anomalies by ADU
4. Trust table updated periodically
5. Secure multi-hop route formed to base station
6. Malicious nodes isolated; packets rerouted dynamically

VIII. SIMULATION & PERFORMANCE EVALUATION

Simulation performed using NS2/NS3 environment.

Parameter	Value
Nodes	100
Area	800m × 800m
Traffic	CBR 512 bytes
Mobility	Random waypoint
Comparison Protocols	LEACH, SEER, SVELTE
Metrics	PDR, Energy, Latency, Detection rate

8.1 Packet Delivery Ratio (PDR)

HLSRF improved delivery by ~14% over LEACH and 9% over SEER under selective forwarding.

8.2 Energy Consumption

Adaptive CH rotation reduced energy depletion by ~11.5%.

8.3 Attack Detection Accuracy

Trust + anomaly combined achieved 92% malicious node detection, outperforming single-layer IDS.

8.4 Network Lifetime

Lifetime extended by ~18% relative to existing secure routing schemes.

Results validate the efficiency of the proposed method.

IX. DISCUSSION

The proposed HLSRF demonstrates balanced security with minimal overhead. The hybrid design prevents both outsider and insider threats, while the session-key mechanism ensures confidentiality. Trust reinforcement effectively mitigates selective forwarding and Sybil behaviour. Energy-aware routing prolongs operational lifetime—critical for remote deployments.

However, real-world testing is still needed. Scaling beyond 1000 nodes and evaluating under mobility-intensive scenarios like battlefield WSNs will further strengthen applicability.

X. CONCLUSION

Secure routing remains one of the most complex yet critical needs of wireless sensor networks. Existing solutions either focus solely on cryptography or trust-based models, often ignoring lightweight design constraints. This work presented an extensive analysis of routing threats and existing protocols, revealed research gaps, and proposed HLSRF a hybrid lightweight secure routing framework integrating key management, trust evaluation, and anomaly detection. Simulation results show promising improvements in packet delivery, attack resistance, and energy efficiency.

Future enhancement possibilities include integration of machine learning for predictive trust modelling, blockchain-backed integrity validation, and real deployment in large-scale IoT sensor ecosystems.

REFERENCES

[1] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, 2002.

[2] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks, 2003.

[3] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," IEEE Wireless Communications, 2004.

[4] A. Liu and P. Ning, "TinyECC: Elliptic Curve Cryptography for Sensor Networks," ACM TOSN, 2008.

[5] W. Bechkit et al., "A Secure Trust-Based Routing Protocol for WSN," Ad Hoc Networks, 2014.

[6] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the Internet of Things," IEEE Communications Surveys & Tutorials, 2015.

[7] W. Heinzelman et al., "Energy Efficient LEACH," Proc. IEEE HICSS, 2000.

[8] S. Lindsey and C. S. Raghavendra, "PEGASIS Protocol," Aerospace Conference Proceedings, IEEE, 2002.
[9] Y. Wang et al., "Trust-Based Secure Routing for WSNs," Future Generation Computer Systems, 2016.
[10] K. Akkaya and M. Younis, "A Survey on Routing Protocols in WSNs," Ad Hoc Networks, 2005.
[11] S. Zhu et al., "LEAP: Efficient Security Mechanisms for WSNs," ACM CCS, 2003.
[12] H. Chan, A. Perrig, et al., "Random Key Predistribution," IEEE S&P, 2003.
[13] D. Liu and M. Ning, "Improved Key Distribution for Sensor Networks," ACM WiSe, 2003.
[14] M. Saleem et al., "Bio-Inspired Routing in WSNs: A Survey," IEEE Communications Surveys, 2011.
[15] L. Eschenauer, "Key Management Scheme for Sensor Networks," ACM CCS, 2002.
[16] Q. Zhou et al., "Secure and Energy Efficient Routing," Journal of Network and Computer Applications, 2018.
[17] H. Kumar and R. Mishra, "Energy Efficient Secure Routing in WSN," IEEE Access, 2020.
[18] S. Raza et al., "SVELTE: IDS for IoT Networks," IEEE Communications, 2013.
[19] R. Roman et al., "Security in WSNs," Computer Networks, 2011.
[20] J. Lopez and J. Zhou, "Wireless Sensor Network Security A Survey," Computer Communications, 2008.
[21] A. Shabut et al., "Trust Models for WSN Security," IEEE TrustCom, 2015.
[22] M. Raya, J. Hubaux, "Securing Wireless Ad Hoc Networks," IEEE Pervasive Computing, 2007.
[23] F. Amsaad et al., "Blockchain-based Secure Routing for WSN," IEEE IoT Journal, 2021.