IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155105

Detection of Blackhole and Sinkhole Attacks in Wireless Sensor Networks Using a Lightweight Secure Protocol

C. Karthika[1] and Dr. P. E. Irin Dorathy[2]

PG Scholar, Department of Electronics and Communication Engineering,

Government College of Engineering, Tirunelveli, Tamil Nadu, India[1]

Assistant Professor, Department of Electronics and Communication Engineering,

Government College of Engineering, Tirunelveli, Tamil Nadu, India[2]

Abstract: Wireless Sensor Networks (WSNs) are widely used in critical applications such as environmental monitoring, healthcare, and industrial automation, where secure and reliable data transmission is essential. However, due to resource constraints and unattended deployment, WSNs are highly vulnerable to routing attacks such as blackhole and sinkhole attacks. This paper proposes a simple and lightweight trust-based security protocol designed to detect and isolate malicious nodes with minimal computational and communication overhead. The protocol operates in three key stages: neighbour monitoring, trust evaluation, and secure route selection. In the monitoring phase, nodes locally observe the packet forwarding behaviour of their one-hop neighbours. A combined trust score is then computed using forwarding reliability and traffic consistency metrics to accurately identify malicious behaviour. Nodes with low trust scores are isolated through a distributed blacklist mechanism. Finally, secure routing decisions are made by selecting nodes with high trust values and sufficient residual energy, ensuring both reliability and energy efficiency. The proposed approach effectively detects both blackhole and sinkhole attacks while maintaining low overhead, making it suitable for resource-constrained WSN environments.

Keywords: WSN, Secure Routing, Lightweight Protocol, Forwarding Ratio, Malicious Node Detection.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are widely used in applications such as environmental monitoring, healthcare, agriculture, industry, and military systems because they can collect and transmit data efficiently. These networks consist of many sensor nodes with limited energy, processing power, and bandwidth, and they are often deployed in remote environments, making energy efficiency very important for long network operation [1]. At the same time, WSNs are vulnerable to attacks like blackhole, selective forwarding, and sinkhole, which can disrupt communication and reduce performance. Existing approaches either focus only on energy efficiency or only on security, and many introduce high computational overhead and energy consumption [2][3]. To address this issue, this paper proposes a simple and lightweight secure routing protocol that combines both energy efficiency and security. The method monitors node behaviour, evaluates trust using forwarding and traffic patterns, detects malicious nodes, and selects routes using only trusted nodes with sufficient energy, without requiring global network knowledge. The remaining section is organized as follows: Subsection 2 illustrates the literature review subsection 3.1 describes the network model, Subsection 3.2 explains the proposed protocol steps, and Subsection 4 presents the performance analysis.

2. RELATED WORK

The Machine Learning-based Secure Routing Protocol (MLSRP), proposed by Edeh Michael Onyema et al., offers a secure and energy-efficient routing framework using a Multi-Criteria Decision-Making approach for clustering and routing based on energy and network conditions. Its novelty includes zone-based clustering, congestion-aware routing, and lightweight XOR-based cryptography. It improves network lifetime, energy efficiency, and data delivery accuracy, but is limited by static decision-making, lack of adaptability to dynamic attacks, and absence of predictive energy and self-healing mechanisms [4]. The EKD-SOCBA framework, proposed by Adil O. Khadidos et al., ensures secure and energy-efficient communication through lightweight key distribution, integrating Golden Jackal Optimization-based clustering, DS-TEA encryption, and efficient key management. It enhances energy efficiency, security, and communication reliability; however, it lacks adaptability, intelligent learning, predictive energy modelling, and self-healing capabilities, limiting its effectiveness in dynamic environments [5]. The dual-phased hybrid framework proposed

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155105

by Michaelraj Kingston Roberts et al. combines Sailfish Optimization (SFO) and Spotted Hyena Optimization (SHO) to improve energy-efficient cluster-based routing by optimizing clustering and routing processes. It achieves better energy efficiency, network lifetime, and packet delivery ratio, but is constrained by static optimization, lack of adaptability, and absence of security, predictive modelling, and self-healing mechanisms in dynamic and adversarial scenarios [6].

Faridha Banu D. et al. proposed a three-layer framework that integrates Self-Tuned Fuzzy Logic with Adaptive Palm Tree Optimization (APTO), Improved Orbit Optimization Algorithm (IOOA), and a Stackelberg Game-Theoretic Approach (SGTA) to enhance clustering, routing, and load balancing in WSNs. The approach improves energy efficiency, throughput, packet delivery ratio, and network lifetime through adaptive clustering, optimized multi-hop routing, and balanced resource allocation. However, it is limited by reliance on simulation-based validation, lack of real-world dataset evaluation, and absence of advanced learning-based adaptability for highly dynamic and adversarial environment [7]. Navneet Kumar et al. proposed a Hybrid Whale-Ant Optimization Algorithm (WAOA) for energy-efficient routing in Wireless Sensor Networks (WSNs). The approach combines Whale Optimization Algorithm (WOA) for effective cluster head (CH) selection and Ant Colony Optimization (ACO) for optimal routing path discovery, leveraging global exploration and local optimization capabilities. It improves network lifetime, residual energy, and routing efficiency, outperforming existing methods such as MOORP, MMABC, and AZEBR. However, it is limited by the absence of integrated security mechanisms, lack of adaptability to dynamic and adversarial environments, and reliance on simulation-based evaluation without real-world validation [8].

3. PROPOSED SYSTEM

Building upon the above network model, this section presents a lightweight secure routing protocol designed to detect and isolate blackhole and sinkhole attacks while maintaining energy efficiency. Unlike existing trust-based schemes that rely on complex computations or global network knowledge, the proposed protocol operates locally using only neighbour's observations. Each node independently monitors the forwarding behaviour and traffic patterns of its one-hop neighbors, computes a unified trust score, and makes routing decisions based on both trustworthiness and residual energy. The protocol is organized into three sequential steps, as illustrated in Figure 1, ensuring a systematic and low-complexity approach to security in resource-constrained WSN environments.

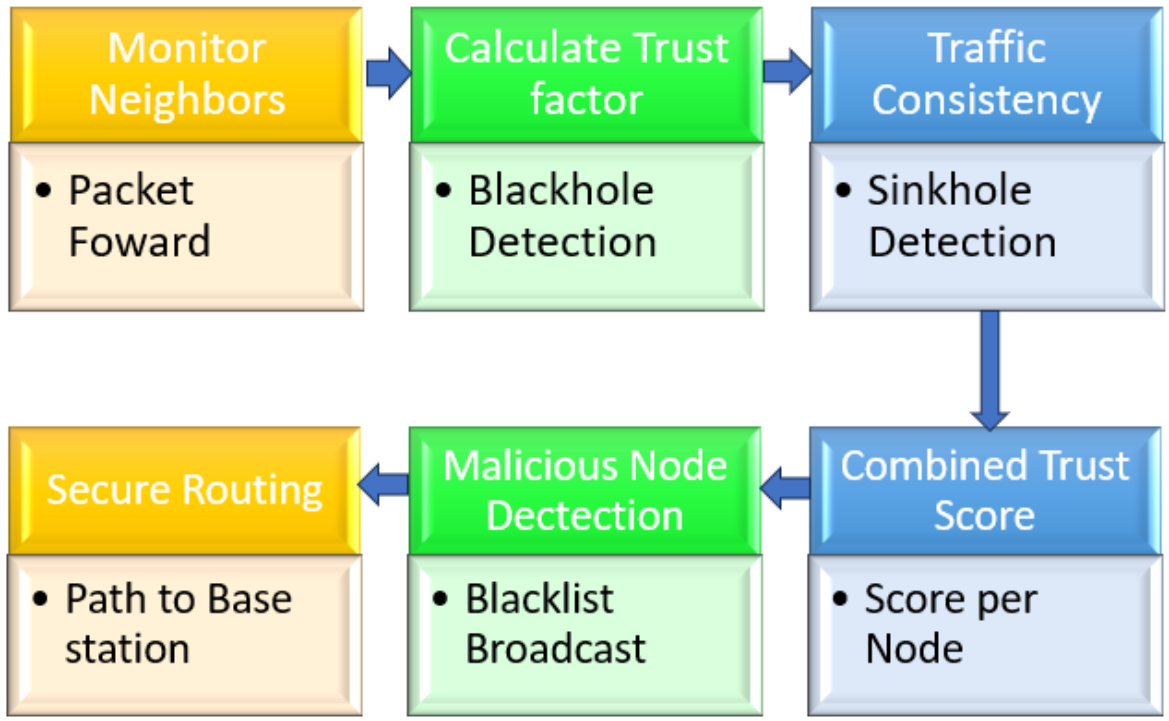

Figure 1: Block diagram of SLSP method

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155105

3.1 Network Model

A wireless sensor network consisting of N homogeneous sensor nodes is randomly deployed over a two-dimensional sensing area. All nodes have identical initial energy and remain static after deployment. A base station (BS) with unlimited energy is located at the edge of the sensing region. Nodes communicate using multi-hop routing.

3.2 Overview of the Proposed Secure Protocol

This paper proposes a simple lightweight trust-based security protocol that operates in three sequential steps. The protocol evaluates node behaviour locally, detects malicious activities, and establishes secure routes without excessive computation or communication overhead.

3.2.1 Neighbour Monitoring

The first step of the proposed protocol is neighbour monitoring, which forms the basis for trust evaluation. Due to limited communication range and energy constraints in wireless sensor networks, a node cannot observe all other nodes. Therefore, each node monitors only its one-hop neighbours, ensuring low overhead and good scalability. Each node observes the behaviour of its neighbours by checking whether they forward or drop packets. When a node sends a packet to a neighbour, it listens to see if the neighbour forwards it to the next hop. These observations help identify whether a node is behaving normally or maliciously.

For every neighbour j, two values are recorded over a time window T_w:

- $P_{rec}(j)$: number of packets received by node j
- $P_{fwd}(j)$: number of packets forwarded by node j

The monitoring is done using promiscuous mode, where nodes listen to all nearby transmissions. If a forwarded packet is not observed within a certain time, it is treated as dropped. All values are stored locally in a monitoring table. At the end of each time window, these values are used for trust calculation, and then reset for the next cycle. This method avoids extra communication and keeps the protocol lightweight.

3.2.2 Forwarding Trust Evaluation

The forwarding behaviour of each node is evaluated using a Forwarding Trust (FT) metric, which measures how reliably a node forwards the packets it receives. It is defined as:

$$FT_j = \frac{P_{fwd}(j)}{P_{rec}(j)+\epsilon} \tag{1}$$

where $P_{rec}(j)$is the number of packets received by node j, $P_{fwd}(j)$is the number of packets it forwards, and $\epsilon = 0.01$avoids division by zero. A well-behaved node forwards most of its packets, resulting in a trust value close to 1, while a malicious node, such as a blackhole attacker, drops packets and produces a value close to 0. Grayhole nodes show intermediate values due to selective forwarding. In practice, if the trust value falls below 0.3, the node is considered suspicious and likely to be malicious, as such low forwarding behaviour indicates intentional packet dropping rather than normal network conditions.

3.2.3 Traffic Consistency Analysis

The protocol detects sinkhole attacks using a Traffic Deviation (TD) metric, which measures how much a node's traffic differs from the network average:

$$TD_j = \frac{|TL_j - \mu_{TL}|}{\mu_{TL}+\epsilon} \tag{2}$$

where $TL_j$is the traffic received by node j, $\mu_{TL}$is the average network traffic, and ϵprevents division by zero. A sinkhole node attracts unusually high traffic, resulting in a large TD value, while normal nodes have TD values close to zero. If $TD_j > 2.0$, the node is considered a sinkhole suspect.

3.2.4 Combined Trust Evaluation and Malicious Node Detection

The protocol computes a unified Trust Score (TS**)** by combining forwarding trust and traffic deviation to accurately evaluate node behaviour:

$$TS_j = w \cdot FT_j + (1-w) \cdot \big(1 - \min(TD_j, 1)\big) \tag{3}$$

where $w = 0.6$gives higher importance to forwarding behaviour. A higher TS value indicates a reliable node, while a lower value indicates suspicious activity. Nodes are classified using a threshold $T_{th} = 0.5$; if $TS_j < 0.5$, the node is

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155105

considered malicious, otherwise it is treated as normal. Once a node is identified as malicious, it is added to a local blacklist, an alert is shared with neighbouring nodes, and it is excluded from all routing decisions. This ensures fast and lightweight isolation of malicious nodes without requiring complex control mechanisms.

3.2.5 Secure Route Selection

During route discovery, only nodes with $TS_j \geq T_{th}$ are selected as forwarders. The next hop is chosen by maximizing trust and residual energy.

$$\text{Next Hop} = \arg\max \left(TS_j \cdot \frac{E_{res}(j)}{E_{init}} \right) \tag{4}$$

This ensures secure and energy-efficient routing. If no trusted neighbour is available, the node either transmits directly or initiates a new route discovery after a delay.

The Figure. 2 presents the flowchart of the proposed 6-step secure routing protocol. The protocol operates in an iterative manner, where each node continuously monitors its neighbors forwarding behaviour.

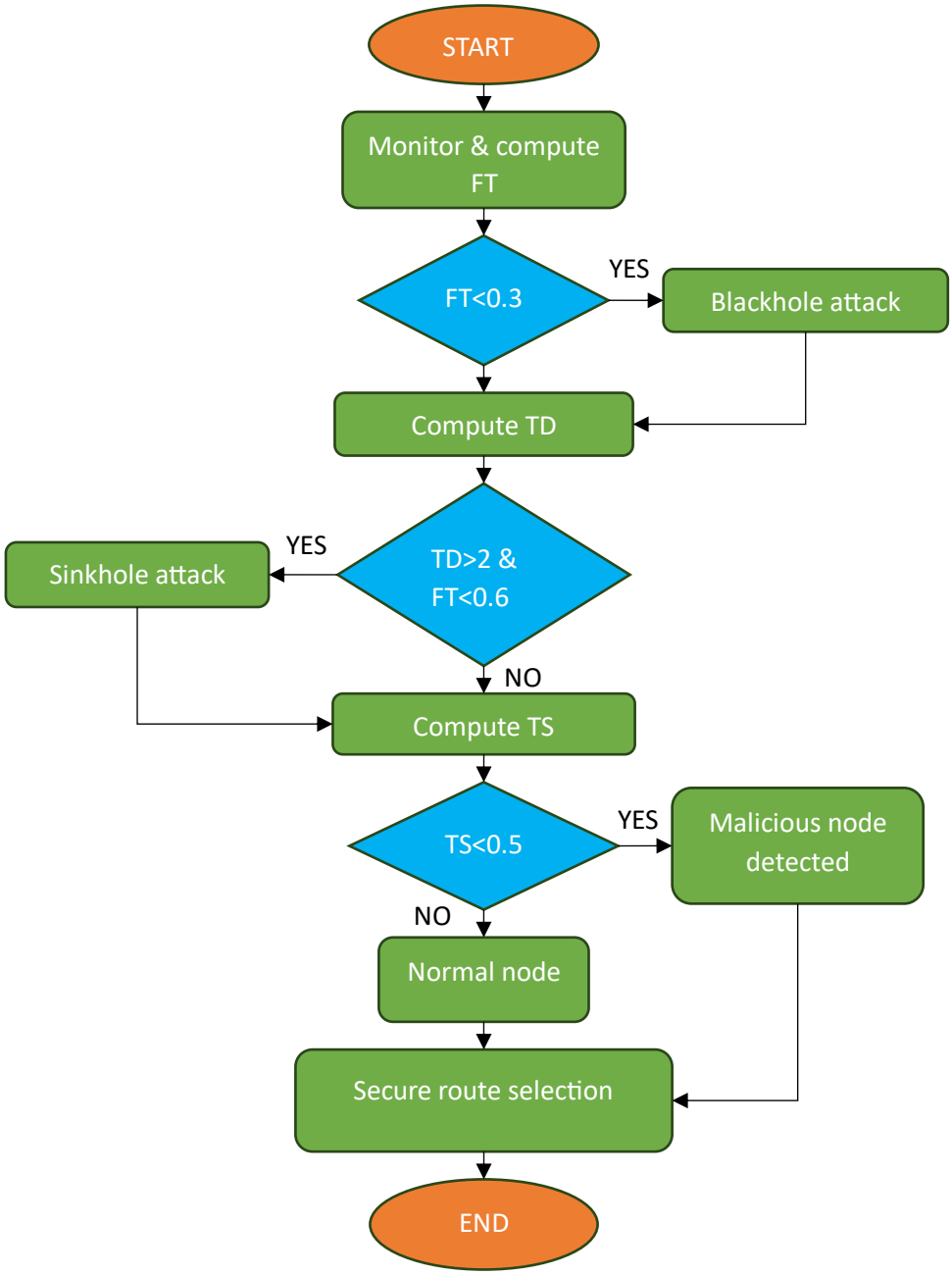

Figure 2: Flow chart of SLSP method

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155105

4. PERFORMANCE EVALUATION AND RESULTS ANALYSIS

4.1 Simulation Setup and Environment

The proposed AARS-DRL protocol is evaluated using MATLAB simulations on a Wireless Sensor Network with 100 nodes deployed over a 200×200 m² area, with the base station at the centre. Each node starts with 2 J of energy, and the simulation runs for 350 rounds using a first-order radio energy model. Nodes have a communication range of 50 m and transmit 4000-bit packets per round. A total of 15 malicious nodes is introduced from the 75th round to test performance under attack conditions. The proposed method is compared with the existing TRUST protocol for performance evaluation.

4.2 Performance Metrics

The performance of the proposed routing protocol is evaluated using three key metrics that collectively capture both network efficiency and security effectiveness.

1. Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is the percentage of data packets successfully delivered from source nodes to the base station. It quantifies the reliability of the routing protocol and is calculated as:

$$PDR = \frac{Packets\ Received\ at\ BS}{Packets\ Sent\ by\ Sources} \times 100\%$$

Higher PDR values indicate superior protocol performance and lower packet loss due to attacks or network congestion.

2. End-to-End Delay

End-to-End Delay is the average time elapsed from when a packet is generated at the source node until it is successfully received at the base station. It is calculated as:

$$End\text{-}to\text{-}End\ Delay = \frac{\sum(Arrival\ Time - Send\ Time)}{Total\ Packets\ Received}$$

Lower delay indicates more efficient routing and faster data delivery.

3.Control Overhead

Control Overhead is defined as the ratio of the total number of control packets transmitted in the network to the total number of packets (control + data) transmitted. Control packets include route request (RREQ), route reply (RREP), hello messages, trust notifications, and blacklist updates that are necessary for route establishment and maintenance but do not carry actual sensed data. Control overhead is mathematically expressed as:

$$Control\ Overhead = \frac{Control\ Packets}{Control\ Packets + Data\ Packets} \times 100\%$$

Lower control overhead indicates more efficient routing with less management traffic.

4.3 Results and Discussion

The performance of the proposed SLSP protocol is evaluated against an existing trust-based protocol (TRUST) using three critical performance metrics, including Packet Delivery Ratio (PDR), End-to-End Delay and Control Overhead. The comparative results are presented from Fig. 3 to Fig 5. The results clearly demonstrate that the proposed SLSP protocol consistently outperforms the baseline method across all evaluated metrics.

Packet delivery ratio

The figure. 3 compares the PDR performance of the proposed SLSP protocol against the existing TRUST protocol across three phases. The existing TRUST protocol achieves 87.9%, 34.1%, and 58.5%, respectively as shown in the figure. The rapid detection of malicious nodes using FT < 0.3 for blackhole attacks and TD > 2.0 with FT < 0.6 for sinkhole attacks minimizes packet loss during the attack period.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155105

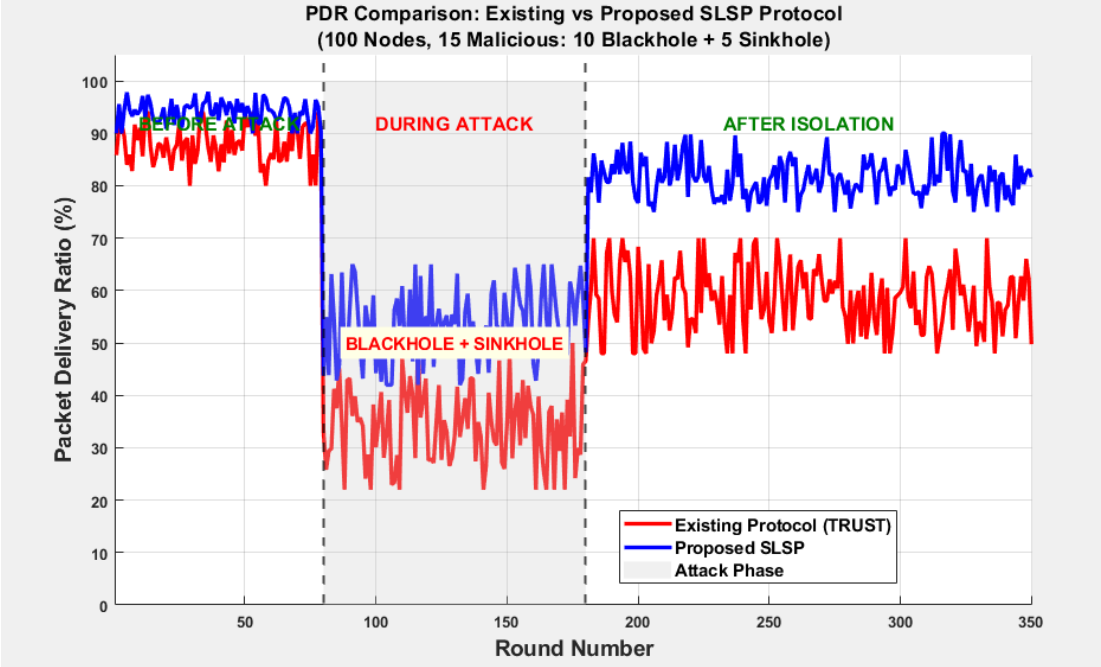

Figure 3: PDR comparison analysis

As summarized in Table 1, SLSP achieves an average PDR of 94.1% before attack, 53.4% during attack, and 81.5% after isolation.

Phase	Existing TRUST	Proposed SLSP	Improvement
Before Attack	87.9%	94.1%	+6.2%
During Attack	34.1%	53.4%	+19.3%
After Isolation	58.5%	81.5%	+23.0%
Overall	60.2%	76.3%	+16.1%

Table 1: PDR improvement of SLSP protocol

End to End delay

The Figure 4 compares the end-to-end delay performance of the proposed SLSP protocol against the existing TRUST protocol over 350 simulation rounds. As shown in the figure, SLSP consistently achieves lower delay across all three phases.

During Attack, TRUST experiences a dramatic delay increase to 0.27 seconds due to frequent route rediscoveries caused by blackhole and sinkhole attacks. In contrast, SLSP maintains delay at only 0.16 seconds. After Isolation, SLSP quickly recovers to 0.09 seconds, while TRUST only recovers to 0.15 seconds due to undetected sinkhole nodes remaining active in the network.

Control overhead

The Figure 5 compares the control overhead of the proposed SLSP protocol against the existing TRUST protocol. The existing TRUST protocol exhibits a control overhead of 27.3%, meaning that more than one-quarter of all network traffic consists of management packets rather than actual data. In contrast, the proposed SLSP protocol achieves significantly lower control overhead at 17.2%, representing a 37.0% relative reduction.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155105

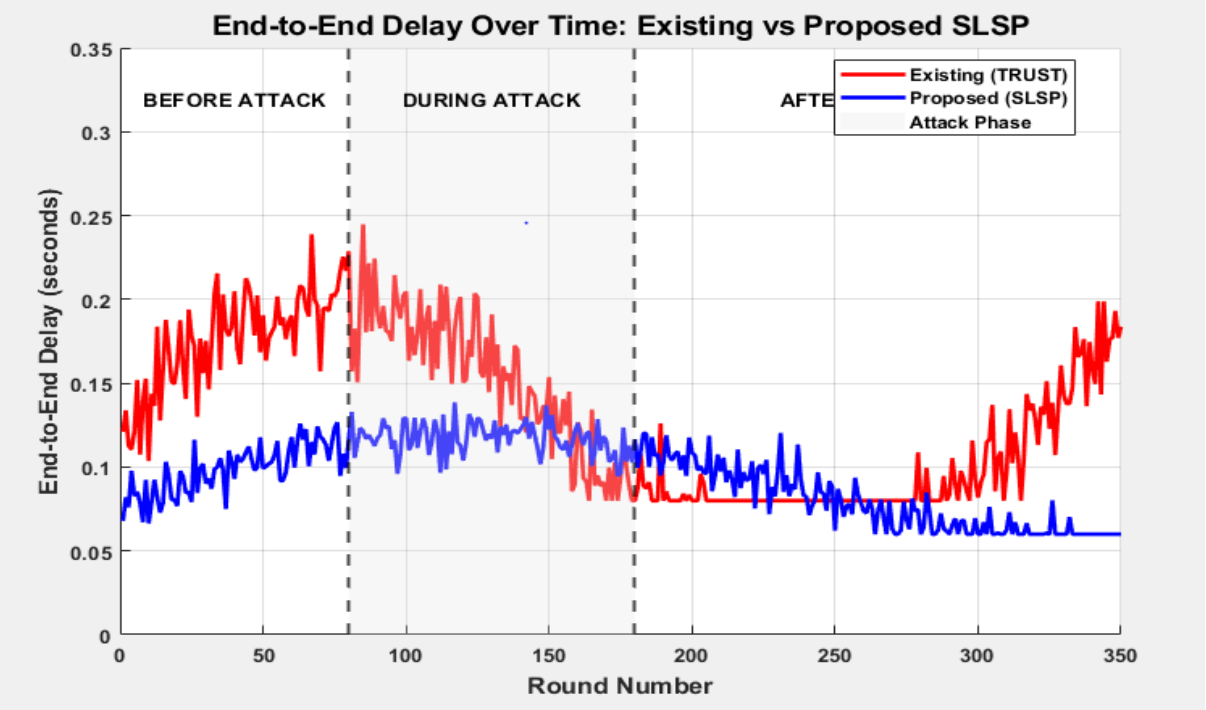

Figure 4: End to End delay analysis

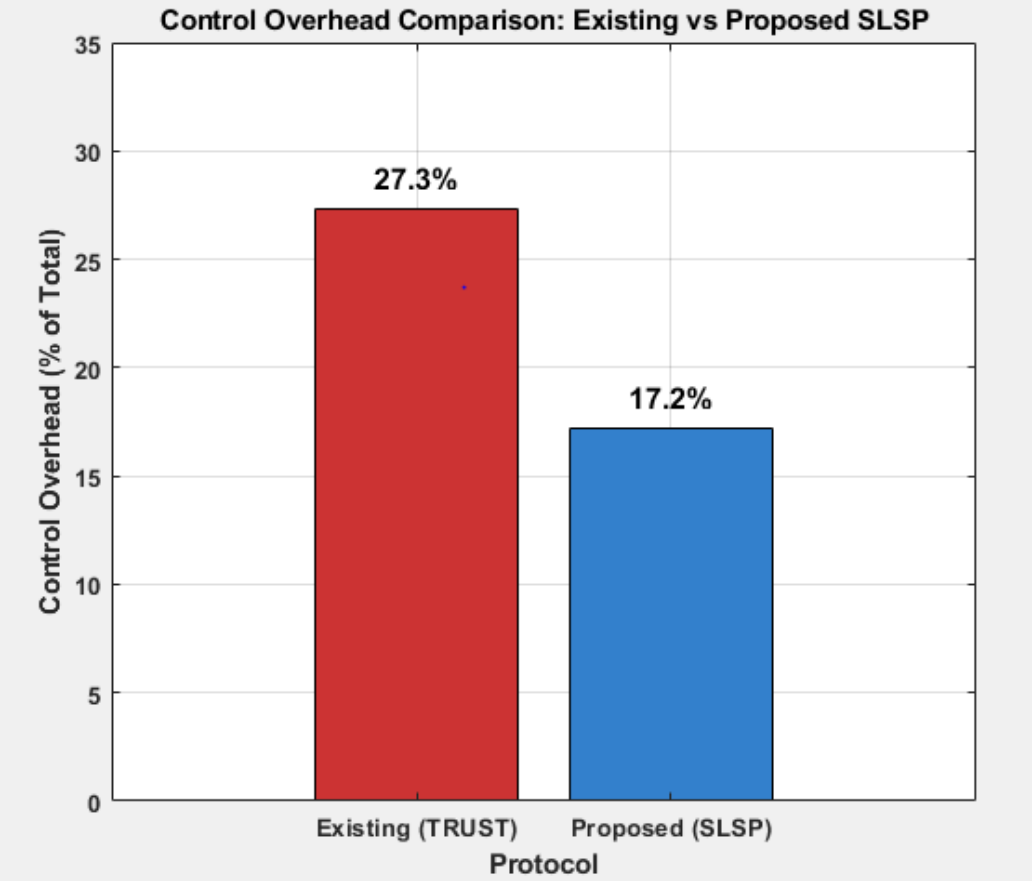

Figure 5: Control overhead comparison

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155105

5. CONCLUSION

This paper proposed a Simple Lightweight Secure Protocol (SLSP) for wireless sensor networks to detect and isolate blackhole and sinkhole attacks while maintaining energy efficiency. The protocol operates in the given sequential steps: neighbors monitoring, forwarding trust evaluation, traffic consistency analysis, combined trust score calculation, malicious node detection, and secure route selection. The performance of SLSP was comprehensively evaluated against an existing trust-based protocol (TRUST/TBSEER) using five critical metrics. The experimental results demonstrate that the proposed SLSP protocol consistently outperforms the baseline protocol across all evaluated metrics. In terms of Packet Delivery Ratio, SLSP achieves 94.1% before attack, maintains 53.4% during attack compared to 34.1% for TRUST, and recovers to 81.5% after isolation compared to 58.5% for TRUST, representing a 56.5% improvement during the critical attack phase. The End-to-End Delay analysis shows that SLSP maintains lower delay throughout all phases, with peak delay of only 0.16 seconds during attack compared to 0.27 seconds for TRUST, a 41% reduction. The Control Overhead of SLSP is measured at 17.2%, significantly lower than the 27.3% overhead of the baseline protocol, representing a 37% relative reduction. This improvement is attributed to SLSP's lightweight design choices like local monitoring eliminates global trust broadcasts, reduced HELLO message frequency lowers periodic traffic, and single-hop blacklist notifications prevent network-wide flooding.

Future work will focus on extending SLSP to detect additional attack types including wormhole, Gray hole, and selective forwarding attacks. Integration of machine learning techniques for adaptive threshold optimization and extension to mobile WSN scenarios are also planned. Furthermore, hardware implementation on real sensor motes will be pursued to validate practical feasibility.

REFERENCES

[1]. A. Ojha and B. Gupta, “Evolving landscape of wireless sensor networks: A survey of trends, timelines, and future perspectives,” *Discover Applied Sciences*, Jul. 2025.
[2]. K. S. Adu-Manu, E. Amoako, and F. Engmann, “Advancements in Machine Learning-Enhanced Green Wireless Sensor Networks: A Comprehensive Survey on Energy Efficiency, Network Performance, and Future Directions,” *Journal of Sensors*, vol. 2025, doi: 10.1155/js/5242517.
[3]. R. Sudha and M. Premkumar, “Securing wireless sensor networks: A survey of challenges and innovations,” *Franklin Open*, vol. 14, 2026.
[4]. E. M. Onyema, S. K. Suguna, B. Sundara vadivazhagan, R. H. Jhaveri, U. N. Esther, E. C. Deborah, and K. Shantha Kumari, “A secure routing protocol for improving the energy efficiency in wireless sensor network applications for industrial manufacturing,” *Next Energy*, vol. 7, 2025.
[5]. A. O. Khadidos, N. Alhebaishi, A. O. Khadidos, M. Altwijri, A. G. Fayoumi, and M. Ragab, “Efficient key distribution for secure and energy-optimized communication in wireless sensor network using bioinspired algorithms,” *Alexandria Engineering Journal*, vol. 92, pp. 63–73, Apr. 2024.
[6]. M. K. Roberts, J. Thangavel, and H. Aldawsari, “An improved dual-phased meta-heuristic optimization-based framework for energy efficient cluster-based routing in wireless sensor networks,” *Alexandria Engineering Journal*, vol. 101, pp. 306–317, Aug. 2024.
[7]. F. B. D. and K. N., “Enhancing wireless sensor network performance through self-tuned fuzzy logic, adaptive palm tree optimization, and Stackelberg game-theoretic load balancing: A comprehensive approach for energy efficiency, reliability, and security,” *Egyptian Informatics Journal*, vol. 32, Dec. 2025.
[8]. N. Kumar, K. Singh, and J. Lloret, “WAOA: A hybrid whale-ant optimization algorithm for energy-efficient routing in wireless sensor networks,” *Computer Networks*, vol. 254, Dec. 2024.

