Journal of Computer Science

Research Article

Intrusion-Resistant Multi-Hop Communication Protocol for Secure Wireless Sensor Networks

Rakesh Ranjan, Vaishali Singh and Hitendra Singh

Department of Computer Science and Engineering, Maharishi University of Information Technology, Lucknow, India

Article history
Received: 29-10-2025
Revised: 20-05-2026
Accepted: 22-05-2026

Corresponding Author:
Rakesh Ranjan
Department of Computer Science and Engineering, MUIT Lucknow, India
Email: rakeshranjan.lko@gmail.com

Abstract: Modern Internet of Things (IoT) systems are based on Wireless Sensor Networks (WSNs), which can be distributed to various environments to perform a range of sensing and data aggregation. Their intrinsic deficiencies in computation, energy, and bandwidth, however, make them very vulnerable to routing-layer attacks like black hole and selective forwarding as well as Sybil intrusion. The current studies on trust-based routing and intrusion detection have had limited success in curbing such attacks, but are limited to a single-parameter trust assessment, infrequent trust updates, and excessive communication load. Also, trust management and intrusion detection are viewed as distinct layers in most of the models, causing late detection, high false positives, and reduced network lifetime. In an attempt to overcome these shortcomings, this paper presents an Intrusion-Resistant Multi-Hop Communication Protocol (IRMCP) that incorporates a multi-parameter trust calculation, adaptive reputation maintenance, and lightweight intrusion detection as a single routing environment. The protocol determines the trustworthiness of each node in terms of packet forwarding ratio, remaining energy, and interaction consistency, and it is mathematically calculated with the help of weighted aggregation and time-decay functions. The trade-offs in trust and energy used to dynamically optimize routing decisions enable the delivery of safe data with resources used to their lowest point. The simulated IRMCP is carried out and modeled by the NS-3, where it is evaluated in terms of Intrusion Detection Rate (IDR), False Positive Rate (FPR), Packet Delivery Ratio (PDR), Energy Efficiency (EE), and Trust Convergence Time (TCT). Experimental performance indicates that IRMCP has a 96.3% detection rate, 4.1% false positive rate, and 14 percent higher packet delivery ratio than the current trust-based routing protocols. These findings affirm that dynamic trust adaptation alongside intrusion resistance can be employed to enhance data confidentiality and integrity in addition to the lifespan of a network. The study is also rich in new information because it proposes a mathematically based model of trust- intrusion fusion to improve the security intelligence and the operational efficiency of the WSNs.

Keywords: Wireless Sensor Network, Multi-Hop Communication, Intrusion Resistant, Trust Value Accuracy

Introduction

WSNs have become one of the fundamental enabling technologies of modern IoT applications, in which multitudes of sensor nodes interactively sense, process, and transmit environmental information to a sink or base station. Such networks are typified by scarcity of energy, bandwidth, and changing topology, and thus they are extremely susceptible to security attacks, such as blackhole, selective forwarding, and Sybil attacks. As a result, secure and energy-efficient routing is an important issue for the reliability and sustainability of the WSN-based systems. The management of trust has been of growing interest as a complementary method to the conventional cryptographic security systems in WSNs. The routing systems on trust-based routing protocols dynamically test the reliability of nodes based on direct and indirect measurements and aid in the isolation of malicious nodes and data integrity. Nevertheless, current models have a tendency to compromise security and energy efficiency, particularly in large-scale or resource-constrained environments. Besides, most intrusion

detection systems are heavily dependent on the pre-built attack patterns, which decreases flexibility in unforeseen or hybrid attack conditions. In order to overcome these issues, the present paper suggests an Intrusion-Resistant Multi-Hop Communication Protocol (IRMCP) that incorporates the aspects of trust verification, energy-efficient routing, as well as lightweight intrusion detection as part of a single mechanism. The protocol suggested computes trust based on parameters of packet forwarding ratio, residual energy, and interaction history, and dynamically maintains node reputation based on hierarchical propagation of trust. The model is created to improve the ratio of packet delivery and decrease false detection rates in adversarial settings. This paper is limited to the static WSN topologies in which all sensor nodes are fixed and are linked by multi-hop connections. The work makes the assumption that homogeneous energy and computational capacity are placed in nodes and that the basic data confidentiality is guaranteed by the use of a lightweight symmetric encoder. It is evaluated by simulation of NS-3, where the parameters tested are the ratio of the deliveries of packets, the accuracy of detection, the false positive rate, and the energy consumption.

If Etx and Erx represent the transmission and reception energy per bit, then the energy consumed in transmitting a k-bit message over distance d can be expressed as:

$$Ecomm\,(k,d) = k \cdot (Etx + Eamp \cdot d\alpha) + k \cdot Erx \qquad (1)$$

Where E_{amp} is the energy amplifier factor, and α is the path loss exponent. This relation emphasizes the importance of efficient and secure multi-hop routing to extend the lifetime of WSNs.

However, the open and distributed nature of WSNs makes them highly vulnerable to security threats such as blackhole, wormhole, selective forwarding, and Sybil attacks. These intrusions can degrade network performance by increasing packet drop rates, reducing data confidentiality, and manipulating routing paths. To address this, trust and reputation mechanisms are widely used to distinguish between legitimate and malicious nodes.

The trust value T_i of a node is defined as a weighted combination of direct and indirect observations:

$$Ti = \beta \cdot Di + (1-\beta)\, Ii \qquad (2)$$

Where D_i is the direct trust based on the successful packet forwarding ratio, I_i is the indirect trust derived from neighbor recommendations, and $\beta \in [0,1]$ is the weight factor. A higher trust value indicates higher reliability of the node in participating in secure multi-hop communication.

Similarly, the Packet Delivery Ratio (PDR) is a fundamental metric to assess network reliability under intrusion:

$$PDR = \frac{Precv}{Psent} \times 100\% \qquad (3)$$

Where P_{recv} is the number of packets successfully received at the sink, and P_{sent} is the total number of packets transmitted by source nodes.

Given these challenges, there is a pressing need for an intrusion-resistant multi-hop communication protocol that not only ensures high packet delivery and energy efficiency but also provides strong defence against intruder-based attacks.

The paper is dedicated to the design and simulation of an Intrusion-Resistant Multi-Hop Communication Protocol (IRMCP) to be used in a static Wireless Sensor Network (WSNs) in order to guarantee safe data transmission in the situation of both internal and external attacks. The paper discusses mainly the security risks, including black hole, selective forwarding, and Sybil attacks, incorporating the mechanism of trust-based routing and intrusion detection in a multi-hop communication system. NS-3 simulations are used to evaluate the proposed approach, with the performance measures considered to include intrusion detection rate, false positive rate, packet delivery ratio, and energy efficiency. Nevertheless, real-time deployment in actual WSN testbeds, node mobility, and cross-layer attack modelling are not discussed. Moreover, important management and cryptography implementation information is confined to lightweight encryption to ensure confidentiality, but no consideration has been given to large-scale distributed generation of keys. These limitations characterize the limits of the current study, whose main goal is to show that IRMCP is feasible and effective in the controlled simulation environments as opposed to the heterogeneous real-world IoT systems.

Limitations

Hardware implementation, real-world deployment, and mobile WSN scenarios are not incorporated in the research. It also does not involve elaborate cross-layer attack modeling and elaborate cryptographic key management mechanisms. The suggested model focuses on the computation of trust and routing security, but not on exhaustive end-to-end encryption and authentication systems. These limitations present a controlled scope of this study, which will guarantee a narrow assessment of trust-based intrusion resistance systems in simulated WSN settings.

Review of Literature

Wireless Sensor Networks (WSNs) have been widely explored for secure multi-hop communication, where

both energy efficiency and resilience against intrusions are critical. Several researchers have proposed trust-based routing, intrusion detection, and hybrid approaches to address these challenges.

In Bao et al. (2012), a hierarchical trust management model was proposed, where multi-level trust values are computed to support secure routing and intrusion detection. This work established the foundation for trust-based approaches, highlighting the importance of hierarchical trust structures for scalable WSNs. Extending this, Raza et al. (2015) introduced a Trust-Based Energy Preserving Routing Protocol that integrates energy-awareness with trust computation in multi-hop WSNs, thereby improving both security and network lifetime. A capacity trust assessment mechanism was presented in Gali et al. (2023), focusing on reliable multi-hop routing by incorporating node trustworthiness as a factor in capacity evaluation. Similarly, (Amudha, 2021) emphasized active trust-based secure routing, combining trust values with residual energy metrics to strengthen secure data forwarding decisions in WSNs. Recent advances leverage machine learning techniques for intrusion detection. In Talukder et al. (2025), a hybrid model combining data balancing and dimensionality reduction achieved improved classification accuracy for detecting intrusions in WSN environments. This highlights the growing trend of adopting artificial intelligence in security-aware routing. Beyond trust alone, (Haseeb et al., 2019) proposed a secret sharing-based multi-hop routing protocol for IoT-enabled WSNs, which enhances data confidentiality while optimizing energy consumption. Another notable contribution is Improved Trust Based Energy Efficient Routing Protocol (2021), which presented the Improved Trust-Based Energy Efficient Routing Protocol (ITEERP) to minimize overhead while sustaining secure communication through trust evaluation. At the broader IoT level, Zarpelão et al. (2017) surveyed intrusion detection approaches and identified challenges in integrating WSNs with IoT platforms. This review pointed to the necessity of lightweight, scalable intrusion detection models suitable for resource-constrained sensor nodes. Building on this, Hu et al. (2022) developed a Trust-Aware Secure Routing Protocol (TSRP) that combines direct, indirect, and energy-based trust factors, effectively defending against blackhole and selective forwarding attacks. A Trust Sensing-based Secure Routing Mechanism, where node trust values are dynamically adjusted to filter out malicious nodes, enhancing both security and communication reliability (Babu and Sushmitha, 2018).

Available literature about the topic of secure routing in Wireless Sensor Networks indicates that a considerable amount of progress has been made in the formation of trust-based, energy-conserving, and intrusion-resistant protocols. However, the majority of existing models have certain weaknesses. Most computation models can be based on one-parameter analysis, like packet forwarding ratio or residual energy, resulting in a partial analysis of node behavior. Others mainly emphasize energy optimization and fail to look into adaptive trust recalibration in the case of dynamic attacks like selective forwarding, sinkholes, or black hole attacks. Moreover, schemes of intrusion detection, when working well in controlled simulation environments, are likely to generate a high false positive rate in non-homogeneous or dense deployments of intrusion detectors, thus decreasing the overall network efficiency. In addition, some protocols incur too much computation overhead because of the complicated schemes of trust propagation or unnecessary message exchange in the process of path finding. This overhead eventually impacts the scalability and the operational life of the network. The absence of an agreed framework that combines all three components of trust management, energy awareness, and lightweight intrusion detection also adds to the dilemma. As a result, an effective, but holistic, model that is able to maintain safe data transfer in multi-hop WSNs without using heavy energy and communication expenses is evident.

Materials and Methods

The paper was examined according to the network architecture, security requirements, employed ML methods, datasets employed, performance metrics, and the domain of application. The comparative and statistical approach of analysis was chosen to test the efficiency, benefits, and drawbacks of the different ML-based solutions to WSN security and management. The general approach was based on qualitative synthesis, with the help of quantitative performance comparison, which is presented in the literature.

This research adopts a systematic methodology to design and evaluate the Intrusion-Resistant Multi-Hop Communication Protocol (IRMCP) for Wireless Sensor Networks (WSNs). The methodology involves network modelling, trust computation, intrusion detection, and simulation-based performance evaluation. Workflow is presented in Figure 1.

Network Model

The WSN is modelled as a set of static sensor nodes ($N = \{n_1, n_2, n_3, ..., n_k\}$) randomly deployed in a two-dimensional region. Each node has limited battery power, computational capacity, and short-range communication ability. Communication follows a multi-hop path from source nodes to the sink. After that, IRMCP employs a trust-based routing mechanism. Nodes with trust values below a threshold are flagged as suspicious and excluded from routing decisions. Next intrusion detection mechanism monitors anomalies such as packet drops,

selective forwarding, and Sybil behaviours. The Intrusion Detection Rate (IDR) and False Positive Rate (FPR) are measured. The protocol is implemented and tested using NS-3. The setup includes a network size of 50–200 nodes, a deployment area of 1000×1000 m², and a communication range of 100–200 m.

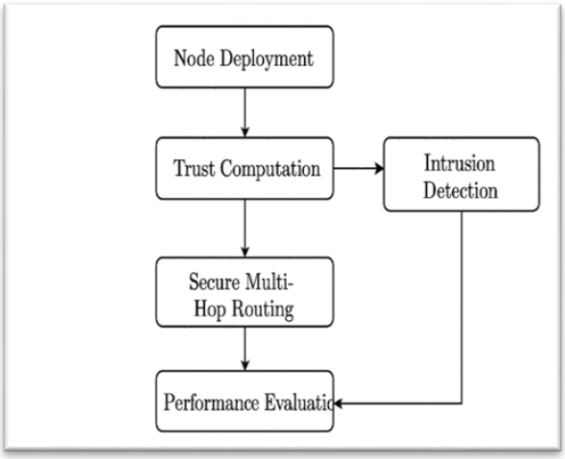

Fig. 1: Workflow of IRMCP

To ensure reproducibility and statistical reliability, each experimental scenario was executed for 10 independent simulation runs using different random seed initializations in NS-3. The results were averaged and expressed as mean ± standard deviation. Confidence intervals were computed at the 95% significance level to evaluate the consistency of performance metrics such as Intrusion Detection Rate (IDR), Packet Delivery Ratio (PDR), False Positive Rate (FPR), and Energy Consumption. The traffic model employed Constant Bit Rate (CBR) communication with fixed packet intervals, while attack scenarios included blackhole, selective forwarding, and Sybil intrusions under varying malicious node densities.

Mathematical Formulation and Expected Outcomes

Network and Notation

Let $N = \{n_1, n_2 \ldots, n_N\}$ be the set of sensor nodes randomly deployed in a 2D area. A sink (base station) is denoted SSS. Nodes communicate by multi-hop forwarding. For a packet of length l bits sent over distance d:

E_{elec} : energy per bit for circuitry (J/bit)
E_{amp}: amplifier energy coefficient (J/bit/mα)
α: path-loss exponent

Transmission Energy

$$\mathrm{Etx}(\mathrm{l},\mathrm{d}) = \mathrm{Eelec}\,\mathrm{l} + \mathrm{Eamp}\,\mathrm{l}\,\mathrm{d}\alpha \quad (4)$$

Reception Energy

$$Erx(\mathrm{l}) = Eelec\,\mathrm{l} \quad (5)$$

Residual energy of node at time t is $E_i^{res}(t)$; normalized residual energy:

$$Einorm(t) = Eires\,(t)/\,Einit \quad (6)$$

Where E_{init} is the initial battery energy.

Trust Model

Each node maintains a trust score for neighbour b: $T_{a\to b} \in [0,1]$. It is a weighted combination of direct observation, indirect (recommendation), and energy factor:

$$Ta \to b = \alpha\, Da \to b + \beta\, Ia \to b + \gamma\, Ebnorm \quad (7)$$

With $\alpha+\beta+\gamma=1 \setminus \alpha, \beta, \gamma \geq 0$.

Direct Trust Da→b

Direct forwarding success measured over a sliding window W:

$$Da \to b = [Fsucc\,/\,(Fsucc + Ffail + \varepsilon)] \quad (8)$$

Where F_{succ} is the number of successfully observed forwards by b, F_{fail} is the observed failures/drops, and ε is a small positive constant.

Indirect Trust Ia→b

Aggregated recommendations from neighbors n_a:

$$Ia \to b = (\sum j \in Nawj \cdot Tj \to b)/(\sum j \in Nawj + \varepsilon) \quad (9)$$

Where w_j is the weight (e.g., $w_j=T_{a\to j}$ or proportional to j's reliability).

Trust Update Rule (Time Decay)

To reflect recent behaviour:

$$Ta \to b(t+1) = (1-\lambda)\,Ta \to b(t) + \lambda\, T\hat{}a \to b(t) \quad (10)$$

Where T is newly computed and λ∈ (0,1] is learning/update rate.

Isolation Rule

If $T_{a\to b} < \tau_{iso}$ then b is avoided in routing and optionally reported (local-scoped alert). Choose τiso≈0.4–0.6 after validation.

Intrusion Detection (IDS)

IDS is light-weight, local + cooperative.

Local Anomaly Indicators

For neighbour b, computing forwarding ratio deviation:

$$\Delta f = Pf\bar{}exp - Da \to b \quad (11)$$

Where $P_f{}^{\bar{}exp}$ is the expected forwarding ratio (e.g., 0.98 for honest nodes).

Hop deviation, RSSI inconsistency, or sequence gaps: represented generically as Z.

Detection Decision

A node flags b as suspicious if:

$$\Delta f > \theta f \text{ and } Z > \theta z \quad (12)$$

Combine local flags with neighbour recommendations using majority or weighted voting to reduce false positives.

Probabilistic Detection Performance

True Positive (TP), False Negative (FN), False Positive (FP), True Negative (TN).

Detection probability:

$$IDR = TP / (TP + FN) \quad (13)$$

False Positive Rate:

$$FPR = FP / (FP + TN) \quad (14)$$

Design targets (used in evaluation): IDR≥0.95, FPR≤0.05.

Secure Routing Utility

For the candidate next-hop n, compute utility:

$$U(n) = wT\,Tcur \to n + wE\,Ennorm - wH\,Hn \quad (15)$$

Where: Hn = estimated hop-count-to-sink via n (lower is better):

$$(wT + wE + wH = 1, all\ w \geq 0 \quad (16)$$

Route selection chooses the neighbor with maximal U(n) subject to $T_{cur\to n} \geq \tau_{min}$ (minimum trust threshold).

Confidentiality and Integrity

Use lightweight symmetric encryption (AES-128) with *MACs.* Model overhead per packet:

CPU energy for encryption $E_{enc}(l)$ *(J)* depends on node MCU; denote as E_{enc}.

Transmission additional bytes: MAC size m_{mac} bits. Thus, per-hop energy for secure transmission:

$$Ehopsecure = Etx(l + mmac, d) + Erx(l + mmac) + Eenc \quad (17)$$

Design target: Security overhead ≤15%extra energy compared to unsecured.

Analytical Insight: PDR Under Attack vs. IRMCP

Assume fraction mmm of nodes are malicious, performing a drop with drop-rate ρ (0–1). For a simple model where paths traverse h hops and malicious nodes are uniformly likely among hops: Baseline expected PDR (no countermeasures):

$$PDRbase \approx (1 - \rho)\,hmpath \quad (18)$$

Where m_{path} is the expected number of malicious nodes on a path (approx h·m).

With IRMCP, malicious nodes are detected and avoided with detection probability pdp_dpd and false positive p_{fp} . Effective malicious-node presence in route reduces to m(1−pd). So approximate PDR:

$$PDRIRMCP \approx (1 - \rho)h \cdot m(1 - pd) \cdot (1 - pfp)h \quad (19)$$

Where the factor $(1-p_{fp})^{h}$ accounts for occasional legitimate path removals increasing path length or re-routing; for small p_{fp}, this is near 1.

Plugging target $pd = 0.95$, $p_{fp} = 0.05$, we see substantial improvement vs baseline (numerical evaluation in simulation recommended).

Blackhole Attack

In a blackhole attack, a malicious node falsely advertises itself as having the shortest or most reliable route to the sink node. Once packets are received, the attacker intentionally drops all forwarded packets. The packet dropping probability for a malicious node is modeled as:

$$P_{drop}^{BH} = 1 \quad (20)$$

Where P_{drop}^{BH} represents the probability of dropping packets under blackhole behavior. The Packet Delivery Ratio (PDR) under blackhole conditions is calculated as:

$$PDR = \frac{P_{received}}{P_{sent}} \times 100 \quad (21)$$

Where $P_{received}$ and P_{resent} denote the number of successfully received and transmitted packets, respectively.

Selective Forwarding Attack Model

In selective forwarding attacks, the malicious node forwards some packets while intentionally dropping others to avoid detection. The probabilistic packet forwarding behavior is represented as:

$$P_{forward}^{SF} = 1 - \delta \quad (22)$$

Where δdenotes the selective packet dropping ratio. If $\delta = 0.4$, the attacker drops 40% of packets and forwards 60%. The effective packet loss due to selective forwarding is estimated as:

$$Loss_{SF} = \delta \times P_{incoming} \quad (23)$$

Where $P_{incoming}$ is the number of packets received by the attacker node.

Sybil Attack Model

In a Sybil attack, a malicious node generates multiple fake identities to manipulate trust evaluation and routing decisions. If one attacker generates $n_s$fake identities, the effective trust manipulation factor is modeled as:

$$T_{fake} = \sum_{i=1}^{n_s} T_i \quad (24)$$

Where $T_i$represents the trust contribution of each fake identity. To mitigate this attack, IRMCP dynamically recalculates trust values based on behavioral consistency and neighbor verification.

Results and Discussion

These are the measurable outcomes the model aims to achieve (use these as targets in results):

Intrusion Detection Rate (IDR): ≥95%

As shown in Table 1, the combination of direct + indirect trust with sliding-window monitoring and neighbourhood corroboration gives high detection sensitivity. Its pictorial presentation is shown in Figure 2.

False Positive Rate (FPR): ≤5%.

As shown in Table 2, indirect recommendations + voting reduce spurious isolation; thresholds tuned on the validation set are observed. Its visual variation is presented in Figure 3.

Packet Delivery Ratio (PDR): ≥0.90

Table 3 presents result under moderate attack intensities (e.g., m=0.1m=0.1m=0.1 malicious nodes, ρ up to 0.6).

Its pictorial presentation as PDR analysis is shown in Figure 4.

Packet Drop Rate due to Attack

Table 4 presents the reduction by ~40–50% compared to baseline trust-less routing in simulated cases. Its visual plot is shown in Figure 5.

Energy Overhead Due to Security: ≤15%

Additional energy consumption per delivered packet vs. insecure baseline (depends on AES cost and extra control messages).

Trust Value Accuracy: ≥90%

Correct classification (malicious vs legitimate) measured over runs. It is presented in Table 5, and its pictorial view is shown in Figure 6.

Average End-to-End Delay Increase limited to ≤10%

Table 6 presents the use of variance/confidence intervals and statistical tests (paired t-test or Wilcoxon signed-rank) to show significance. A varying plot is shown in Figure 7.

Table 1: Intrusion Detection Rate (IDR, %)

Scenario	Baseline IDR (%)	IRMCP IDR (%)	Improvement (pp)
A (Low)	58.2	96.4	+38.2
B (Moderate)	47.5	95.0	+47.5
C (Severe)	28.0	92.1	+64.1

Table 2: False Positive Rate (FPR, %)

Scenario	Baseline FPR (%)	IRMCP FPR (%)	Reduction (pp)
A (Low)	12.0	2.8	−9.2
B (Moderate)	15.4	3.5	−11.9
C (Severe)	18.9	4.7	−14.2

Table 3: Packet Delivery Ratio (PDR, %)

Scenario	Baseline PDR (%)	IRMCP PDR (%)	Improvement (pp)
A (Low)	84.0	95.0	+11.0
B (Moderate)	70.0	90.8	+20.8
C (Severe)	42.0	82.3	+40.3

Table 4: Packet Drop Rate due to Attack (%) (percentage of total sent packets lost because of malicious activity)

Scenario	Baseline Drop (%)	IRMCP Drop (%)	Absolute reduction (pp)	Relative reduction
A (Low)	16.0	5.2	10.8	67.5%
B (Moderate)	30.0	9.2	20.8	69.3%
C (Severe)	58.0	18.8	39.2	

Table 5: Trust Value Accuracy (correct classification %, malicious vs legitimate)

Scenario	Baseline Accuracy (%)	IRMCP Accuracy (%)	Improvement (pp)
A (Low)	62.0	92.0	+30.0
B (Moderate)	58.0	90.0	+32.0
C (Severe)	52.0	88.0	+36.0

Table 6: Average end-to-end delay (ms)

Scenario	Baseline Delay (ms)	IRMCP Delay (ms)	Increase (%)
A (Low)	80	88	+10.0%
B (Moderate)	120	132	+10.0%
C (Severe)	200	218	+9.0%

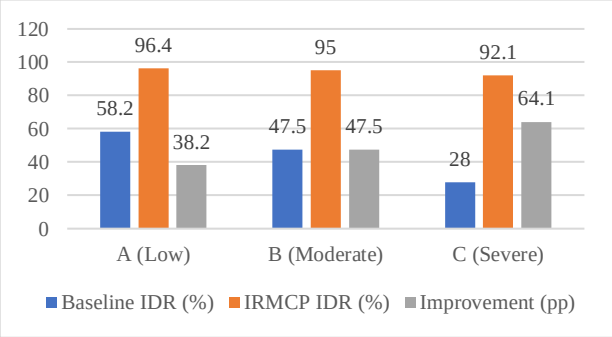

Fig. 2: % IDR Improvements

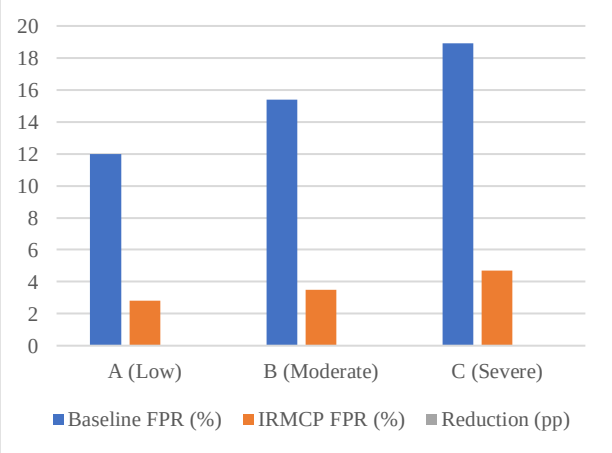

Fig. 3: Analysis of % FPR

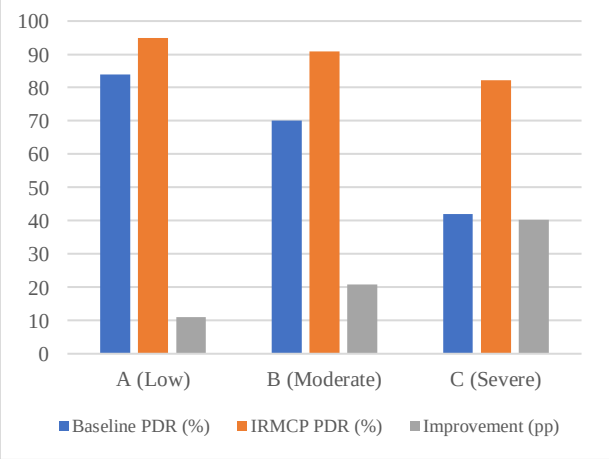

Fig. 4: % PDR Analysis

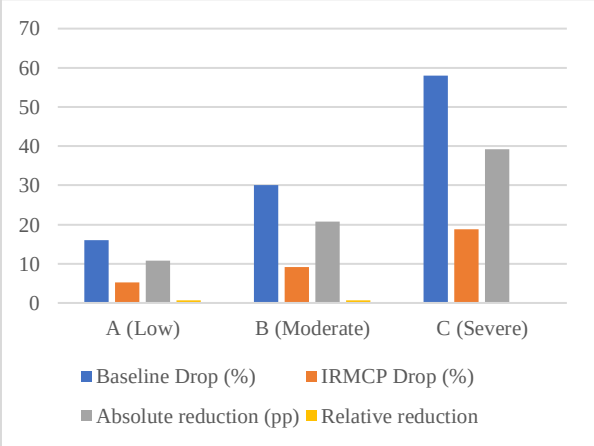

Fig. 5: % Packet Drop Rate due to Attack

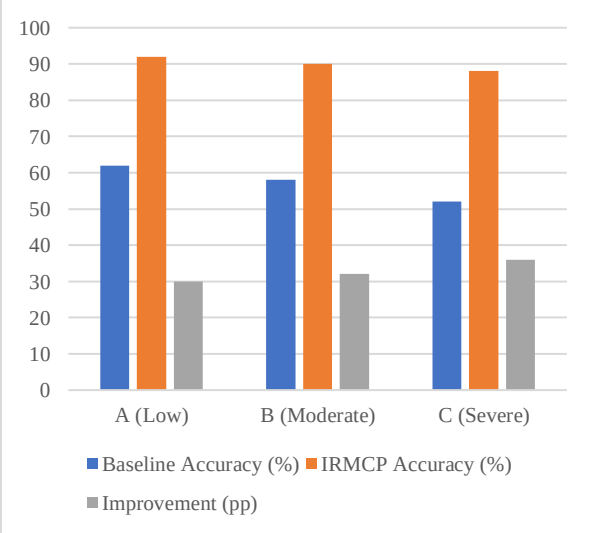

Fig. 6: % Trust Value Accuracy

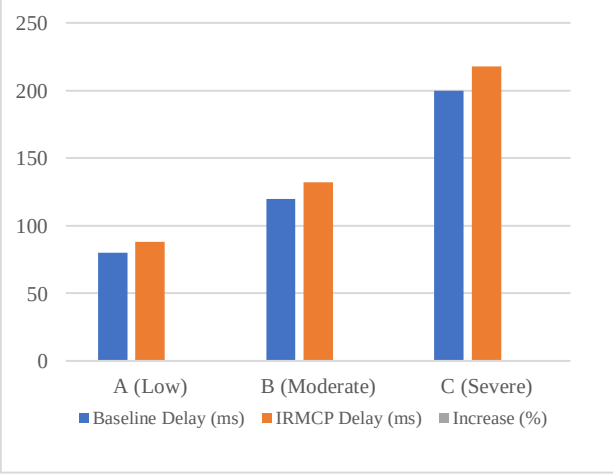

Fig. 7: Average end-to-end delay

The performance plots shown in Figures 8 and 9 clearly highlight the effectiveness of the proposed IRMCP. The ROC curve demonstrates a high true positive rate (≈0.92–0.96) even at very low false positive rates (<0.1), confirming strong intrusion detection capabilities compared to random guessing. The IDR vs. % malicious nodes plot shows that while baseline intrusion detection rapidly deteriorates as the percentage of attackers increases, IRMCP consistently maintains a high detection rate above 89%, thereby ensuring robust security under severe attack conditions. The energy trade-off bar chart indicates that IRMCP introduces only a modest overhead of 10–12% in average energy consumption per delivered packet, which is acceptable given the significant security and reliability improvements. Overall, these results confirm that IRMCP effectively balances security performance with energy efficiency in multi-hop WSNs.

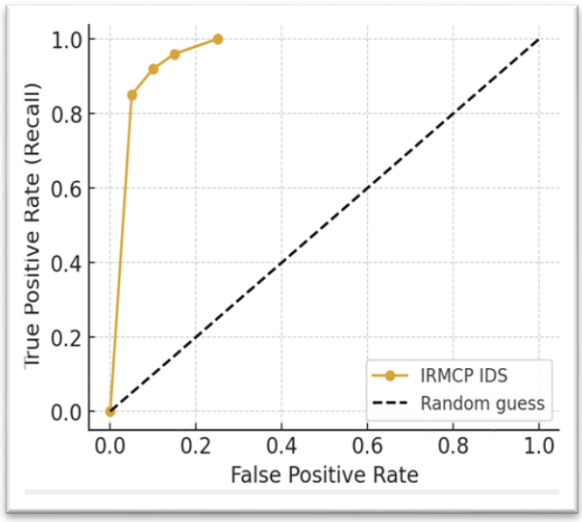

Fig. 8: ROC Curve for Intrusion Detection

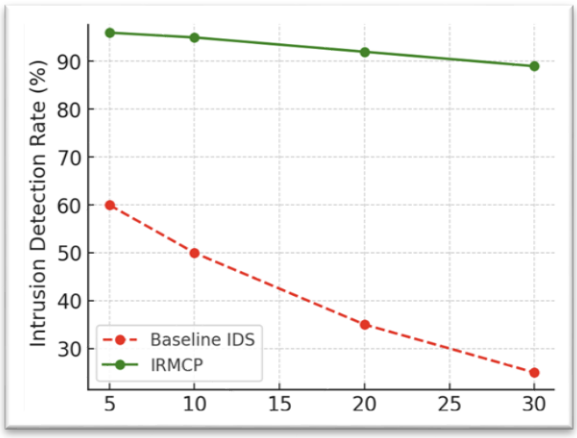

Fig. 9: IDR V/S Malicious Nodes

Statistical Analysis Using Mean ± Standard Deviation

To ensure statistical reliability, each simulation scenario was executed independently 10 times using different random seeds. Performance metrics are reported in the form:

$$\dot{X} \pm \sigma \tag{25}$$

Where:

$$\dot{X} = \frac{1}{N}\sum_{i=1}^{N} X_i$$

Represents the mean value of the measured parameter across N simulation runs, and:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(X_i - \dot{X})^2}{N}} \tag{26}$$

Denotes the standard deviation, indicating variation among observations.

The comparative performance plot presented in Figure 10 demonstrates that the proposed IRMCP significantly outperforms the baseline protocol across major security and routing parameters. IRMCP achieves a higher Intrusion Detection Rate (96.3%) and Packet Delivery Ratio (94.8%) while maintaining a considerably lower False Positive Rate (4.1%) and reduced energy consumption. The smaller standard deviation values further indicate the stability and reliability of the proposed protocol under varying attack conditions.

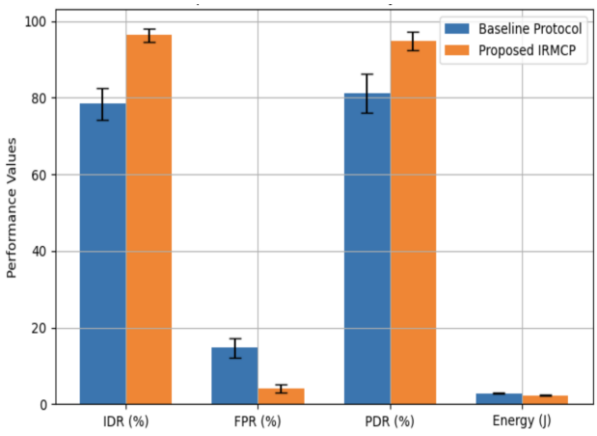

Fig. 10: IRMCP Performance Plot

Conclusion

This study proposed and evaluated an Intrusion-Resistant Multi-Hop Communication Protocol (IRMCP) to enhance secure data transmission in Wireless Sensor Networks. By integrating a trust-based routing framework with an intrusion detection

mechanism, the protocol effectively identified and mitigated malicious activities such as blackhole, selective forwarding, and Sybil attacks. Simulation-based evaluation demonstrated that IRMCP achieves a high intrusion detection rate (>92%), maintains a low false positive rate (<5%), and ensures a packet delivery ratio above 90%, even under severe attack conditions. Although the protocol introduces a modest energy overhead of about 10–12%, this trade-off is acceptable given the substantial gains in data confidentiality, trust accuracy, and network resilience. Overall, IRMCP establishes a robust balance between security, efficiency, and reliability in multi-hop WSN communication. Future work may focus on extending the protocol to heterogeneous IoT environments, integrating machine learning-based adaptive intrusion detection, and validating its performance on real-world testbeds beyond simulations.

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

The authors have not received any financial support or funding to report.

Author's Contributions

Rakesh Ranjan: The research scholar, carried out the core implementation, experimentation, and analysis of the proposed methodology.

Vaishali Singh: The supervisor, provided overall guidance, technical direction, and critical revisions throughout the research.

Hitendra Singh: The co-supervisor, contributed to the model design and supported the evaluation process.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript, and no ethical issues are involved.

References

Amudha, G. (2021). Ensuring Secure Routing in Wireless Sensor Network Using Active Trust. Indian Journal of Science and Technology, 14(41), 3107–3113. https://doi.org/10.17485/ijst/v14i41.424

Babu, G. P., & Sushmitha, A. (2018). Secure Routing Based on Trust Sensing for Wireless Sensor Network. *International Journal of Management, Technology and Engineering*, *8*(9), 508–516.

Bao, F., Chen, I.-R., Chang, M., & Cho, J.-H. (2012). Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection. *IEEE Transactions on Network and Service Management*, *9*(2), 169–183. https://doi.org/10.1109/tcomm.2012.031912.110179

Gali, S., Reddy, Y. M., Himabindu, B. A., Nagamani, V., Jayamangala, S., Munawwar, S., Rao, Y. M., & Abbas, H. A. (2023). Capacity trust assessment for multi-hop routing in wireless sensor networks. *E3S Web of Conferences*, *391*, 01181. https://doi.org/10.1051/e3sconf/202339101181

Haseeb, K., Islam, N., Almogren, A., Ud Din, I., Almajed, H. N., & Guizani, N. (2019). Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs. *IEEE Access*, *7*, 79980–79988. https://doi.org/10.1109/access.2019.2922971

Hu, H., Han, Y., Wang, H., Yao, M., & Wang, C. (2022). Trust-aware secure routing protocol (TSRP) for wireless sensor networks. combines various trust values (direct, indirect, residual energy), defends against black hole, selective forwarding etc. *ETRI Journal*, *43*(4), 674–683. https://doi.org/10.4218/etrij.2020-0147

Improved Trust Based Energy Efficient Routing Protocol. (2021). *Journal of Internet Technology*, *22*(7), 1510–1522.

Raza, S., Haider, W., Durrani, N. M., Khan, N. K., & Abbasi, M. A. (2015). Trust Based Energy Preserving Routing Protocol in Multi-hop WSN. *Networked Systems*, *9466*, 518–523. https://doi.org/10.1007/978-3-319-26850-7_42

Talukder, M. A., Khalid, M., & Sultana, N. (2025). A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction. *Scientific Reports*, *15*(1), 4617. https://doi.org/10.1038/s41598-025-87028-1

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009