



JOURNAL ON COMMUNICATIONS

ISSN:1000-436X

Scopus®

REGISTERED

www.jocs.review

A Lightweight Dynamic Trust-Based Secure Routing Framework for Mitigating Black Hole Attacks in Wireless Sensor Networks

Jyoti Kataria, Dr. Ankit Kumar, Dr. Ganesh Kumar Dixit
Starex University Binola, Gurugram, Haryana, India.

Abstract:

Wireless Sensor Networks (WSNs) have limited resources for energy, compute, memory, and communication; routing security is a particularly challenging design issue. Because an adversary node might draw traffic by promoting an ostensibly advantageous route and subsequently destroy packets rather than forwarding them, Black Hole attacks are disruptive. This research presents a lightweight, dynamic, trust-based routing architecture that links route-selection choices to observations of forwarding behaviour. Attack detection, secure route selection, neighbour monitoring, and trust assessment are all included in the framework. From its forwarding history, each potential neighbour is given a behavioural trust value; nodes whose dependability stays below an adaptive decision threshold are not included in the route creation process. In order to balance network efficiency and security, route selection also takes hop count, residual energy, and forwarding dependability into account. CBR traffic and 100-second simulations are used to construct a repeatable NS-3-based assessment strategy for 50–100 nodes in a 1000 × 1000 m region. Under both normal and Black Hole conditions, the research assesses Packet Delivery Ratio (PDR), throughput, end-to-end latency, energy usage, routing overhead, and detection performance. The PDR ranges in the provided presentation are not measured experimental results; they are only initial goal values. The suggested architecture may be expanded with machine-learning models for adaptive and coordinated-attack detection in order to offer a resource-conscious foundation for safe WSN routing.

Keywords: AODV, trust management, secure routing, intrusion detection, energy efficiency, NS-3, Black Hole Attack

INTRODUCTION

Distributed sensing devices work together in wireless sensor networks to monitor physical occurrences and send measurements to a sink or base station. They are used in surveillance, industrial automation, agriculture, healthcare, and environmental monitoring. In contrast to traditional networks, sensor nodes are frequently limited by radio range, memory, CPU power, bandwidth, and battery capacity. These features make it challenging to implement security measures at scale that call for significant computation or communication.

Since forwarding choices impact whether sensed information reaches the sink, routing is a crucial security layer. Routing manipulation and insider attacks are made possible by the wireless medium, dispersed design, and restricted node capabilities, according to traditional secure-routing research. As a result, trust management has been researched as an additional method for spotting untrustworthy nodes and assisting with safe routing choices.

One especially harmful routing behaviour is a Black Hole attack. By promoting a very alluring way, an attacker tries to join a source-to-destination route. Once chosen, the attacker has the option to discard packets whole or selectively. The ensuing data loss might increase delay and route-recovery traffic while decreasing PDR and throughput.

straightforward forwarding-ratio detector's drawback is that packet loss does not necessarily indicate malevolent activity. Forwarding success can also be decreased by wireless interference, congestion, connection failure, and temporary network circumstances. Therefore,

rather than seeing a single packet loss as evidence of maliciousness, a meaningful trust-based architecture should integrate behavioural evidence with route quality and resource information.

RELATED WORK

- From the viewpoints of protocol, cryptography, intrusion detection, and trust management, security-aware routing in sensor networks has been studied. Routing systems in sensor networks are vulnerable to attacks that alter traffic attraction and forwarding behavior, as Karlof and Wagner showed. Because trust mechanisms let nodes to make judgments about cooperation or routing based on past behaviour, they have since grown in importance as a field of study [1]. Han et al. identified malicious-node detection, safe routing, data aggregation, geolocation, and node selection as crucial trust applications after surveying trust models for WSNs [2]. Additionally, their study highlights the need for a trust model to take into consideration the operational and resource features of WSNs. Momani and Challa's additional analysis emphasized trust management systems best practices [3], While Ahmed and Shi offered a thorough analysis classifying assaults on key management and trust processes [4]. Additionally, secure-routing studies demonstrate that routing characteristics like energy, topology, and communication cost must be taken into account while making security selections These findings inform the suggested approach, which uses trust as a security filter and one element of route quality rather than replacing routing entirely with trust. Perrig et al.'s SPINS for sensor network security is an example of early baseline work in cryptographic protection [5], as well as Deng et al.'s INSENS and other intrusion-tolerant routing protocols [6]. Ganeriwal et al. suggested reputation-based frameworks, like Watchdog mechanisms, for monitoring methods to assess node cooperation [7]. Conti et al. have also investigated distributed anomaly detection systems to deal with node tampering [8]. Energy-efficient trust management for secure devices in wireless contexts is the subject of recent advancements by Chauhan et al. [9], in addition to the cautious rating systems for Maarouf et al.'s trust-enabled routing [10]. Secure geographic routing protocols by García-Otero et al. further confirm that security decisions must be evaluated alongside network topology and communication constraints [11]. Overall surveys on secure WSN routing by Sudha and Premkumar highlight the need to balance security filters with resource awareness [12].

Approach	**Primary idea**	**Typical limitation addressed by proposed work**
Watchdog	Observe next-hop forwarding	Continuous observation can consume energy and may be affected by wireless losses.
IDS-based routing	Detect anomalous network behavior	Additional computation/features may increase resource requirements.
Cryptographic protection	Authenticate/protect messages	Authentication does not by itself guarantee correct forwarding by a compromised authenticated node.

Trust-based routing	Use behavioral evidence to rank/filter nodes	Trust manipulation, threshold selection, and overhead require careful design.
Proposed framework	Dynamic trust + route/resource factors	Designed as a lightweight integrated decision process.

SYSTEM MODEL AND THREAT MODEL

A. Network Model

We consider a multi-hop WSN consisting of static or quasi-static sensor nodes and one sink/base station. Nodes communicate through short-range wireless links and may forward traffic generated by other nodes. Each node maintains local information about its neighboring nodes. Route discovery follows the selected routing protocol, while the proposed trust layer evaluates candidate forwarders.

B. Threat Model

The adversary is assumed to control one or more internal sensor nodes. A Black Hole node participates in route discovery, attempts to attract traffic by advertising a favorable route, and subsequently drops received data packets. The baseline threat considered is a persistent packet-dropping Black Hole. More sophisticated behaviors, including on-off and colluding attacks, are reserved for future evaluation.

C. Assumptions

- Nodes can observe or otherwise verify forwarding events within their communication range.
- Packet-forwarding statistics can be accumulated over a finite observation window.
- Each node can maintain a small trust table for relevant neighbours.
- The trust mechanism itself is not assumed to be cryptographically trusted; its robustness is evaluated through threshold and sensitivity experiments.

PROPOSED TRUST-BASED ROUTING FRAMEWORK

The four logical parts of the suggested architecture are Secure Route Selection, Attack Detection, Trust Evaluation, and Neighbour Monitoring. The elements function as a feedback loop: trust is updated by forwarding observations; trust establishes node eligibility; eligible nodes take part in route scoring; and trust is updated once again by subsequent forwarding behaviour.

A. Neighbor Monitoring

A monitoring node keeps track of how many packets a neighbour accepts for forwarding and how many are later seen to have been successfully forwarded within each observation window. Communication consistency, route-advertisement behaviour, and packet-drop ratio are examples of further evidence. Classifying a node based just on a single transmission failure is avoided by using an observation window.

B. Direct Trust Estimation

The percentage of forwarding chances that lead to successful forwarding is the fundamental forwarding trust for neighbour i:

$$T_i(t) = F_i(t) / \max(R_i(t), 1)$$

where $R_i(t)$ is the number of packets received by node i for forwarding, and $F_i(t)$ is the number of successfully forwarded packets ascribed to node i during the current observation window. Division by zero is prohibited by the max operation. The range of the value is 0 to 1.

An exponentially smoothed update can be used to lessen sudden changes in confidence:

$$\bar{T}_i(t) = \alpha T_i(t) + (1-\alpha)\bar{T}_i(t-1)$$

where the impact of recent observations is controlled by α. A lower α offers more stability against transient losses, whereas a larger α increases the detector's responsiveness.

C. Detection Decision

When a node's smoothed trust value stays below a threshold τ for the necessary decision condition, it is deemed suspicious. The implementation should demand either a minimum number of observations or sequential low-trust windows instead of a single packet event. This lessens false positives brought on by transient channel conditions.

$$\text{Malicious(i)} = 1, \text{ if } \bar{T}_i(t) < \tau; \text{ otherwise, } 0$$

D. Secure Route Selection

Malicious nodes are eliminated from candidate pathways. Security and resource characteristics can be combined in a normalized route score for the remaining routes:

$$S(P) = w_1T(P) + w_2R(P) + w_3E(P) - w_4H(P)$$

where w_1–w_4 are empirically chosen weights, T(P) is the cumulative trust of route P, R(P) is forwarding reliability, E(P) is normalized residual-energy information, and H(P) is normalized hop count. The weights must be reported with the final implementation and justified through sensitivity analysis.

E. Algorithm

1. Initialize the WSN and routing state.
2. Discover candidate routes from source to sink.
3. Monitor forwarding behaviour of candidate next hops.
4. Accumulate received and successfully forwarded packet counts.
5. Calculate current and smoothed trust values.
6. Compare trust against the detection threshold.
7. Temporarily isolate nodes that fail the detection condition.
8. Remove routes containing isolated nodes.
9. Score remaining routes using trust, forwarding reliability, energy, and hop count.
10. Select the highest-scoring eligible route and transmit data.

11. Update trust periodically and repeat the monitoring cycle

Flow of the Proposed Algorithm

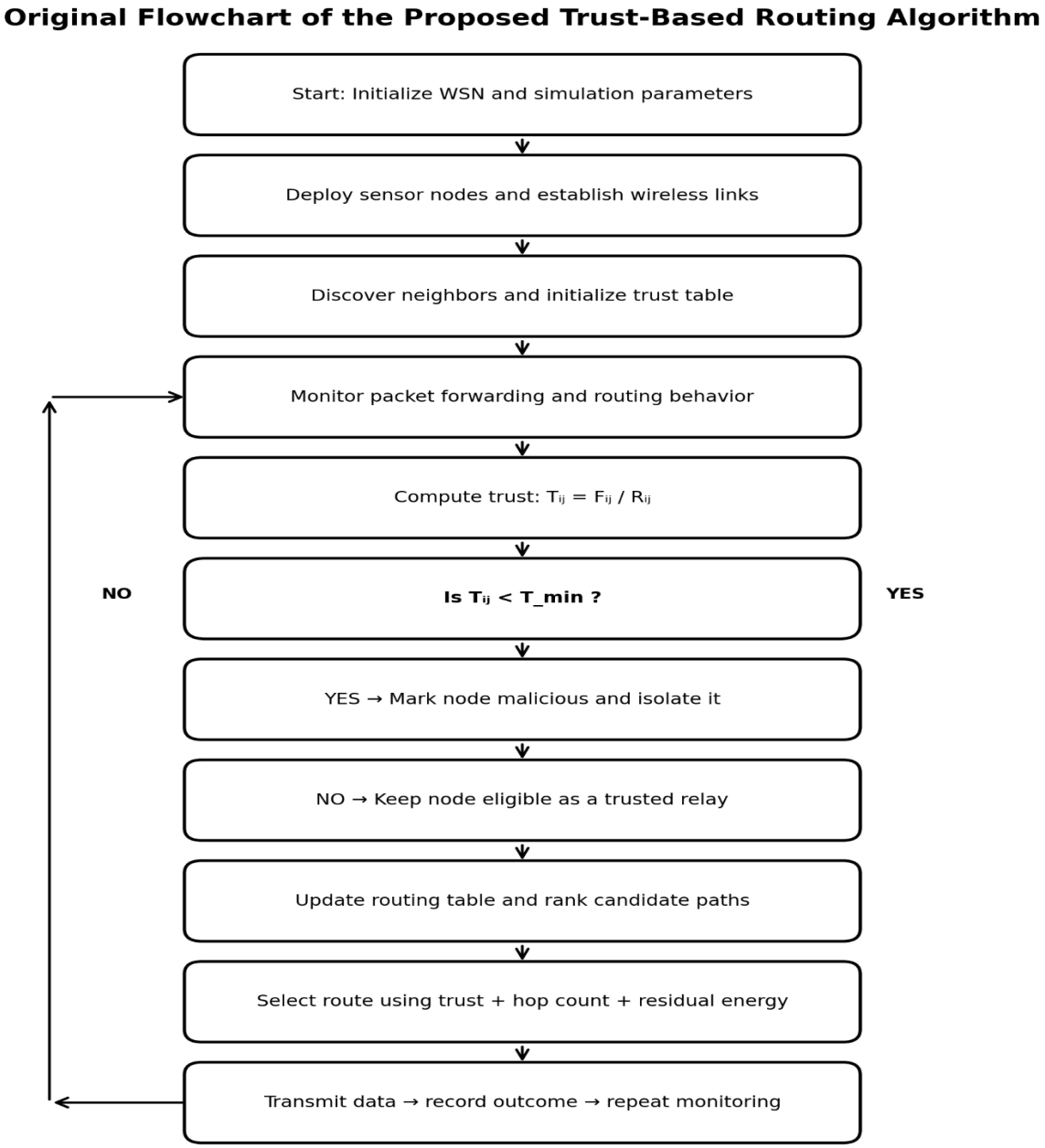


Fig. 2. Original flowchart of the proposed trust-based routing algorithm

Simulation Methodology

The proposed algorithm is intended for implementation in NS-3. The current NS-3 model library includes an AODV implementation based on RFC 3561 and provides an energy framework and Flow Monitor components suitable for performance evaluation [11]. The following parameterization follows the study specification supplied for this manuscript.

Parameter	Value / Setting
Simulator	NS-3
Network area	1000 × 1000 m
Number of nodes	50–100
Transmission range	250 m
Traffic	CBR
Simulation time	100s
Attack scenario	Black Hole node(s)
Baseline protocols	AODV, Watchdog-style monitoring, IDS-based routing
Primary metrics	PDR, throughput, energy, detection accuracy, routing overhead

Performance Metrics

Packet Delivery Ratio (PDR)

PDR = (packets received at destination / packets generated by sources) × 100. Higher PDR indicates more reliable delivery.

Throughput

Throughput measures the useful data successfully delivered to the destination per unit time. Higher throughput indicates better effective network utilization.

Energy Consumption

Energy consumption is measured from node transmission, reception, and idle/processing costs. Lower consumption for the same delivery workload indicates better efficiency.

Detection Accuracy

Detection accuracy should be calculated from true positives, true negatives, false positives, and false negatives using ground-truth attacker identities.

Routing Overhead

Routing overhead quantifies control traffic or routing-control bytes relative to successfully delivered data. Excessive monitoring messages should be avoided in a lightweight approach.

Comparative Analysis

Under the same topology, traffic, mobility, and attack scenarios, the suggested approach should be contrasted with traditional AODV, Watchdog-style forwarding monitoring, and an IDS-based routing baseline. Confidence intervals should be supplied and the comparison should be performed across several random seeds. This is crucial since statistical superiority cannot be shown by a single simulation run.

Method	**Black Hole detection**	**PDR**	**Throughput**	**Energy**	**Overhead**
AODV	Low / attack-unaware	Lower	Lower under attack	Higher due to losses/recovery	Low baseline
Watchdog-style	Moderate	Moderate	Moderate	Moderate–High	Monitoring overhead
IDS-based	High potential	High	High	Higher processing/control cost	High
Proposed trust-based	Target: high	Target: 95–98%	Target: improved	Target: reduced	Target: low

PDR Analysis

An expected/examined PDR range of 80–85% for current techniques and 95–98% for the suggested strategy is reported in the research specification. For the purpose of visualizing the provided comparison, Figure 3 depicts those ranges by their midpoints. Before submitting these numbers as experimental results, the NS-3 experiment's real averages and confidence intervals should be used in their stead.

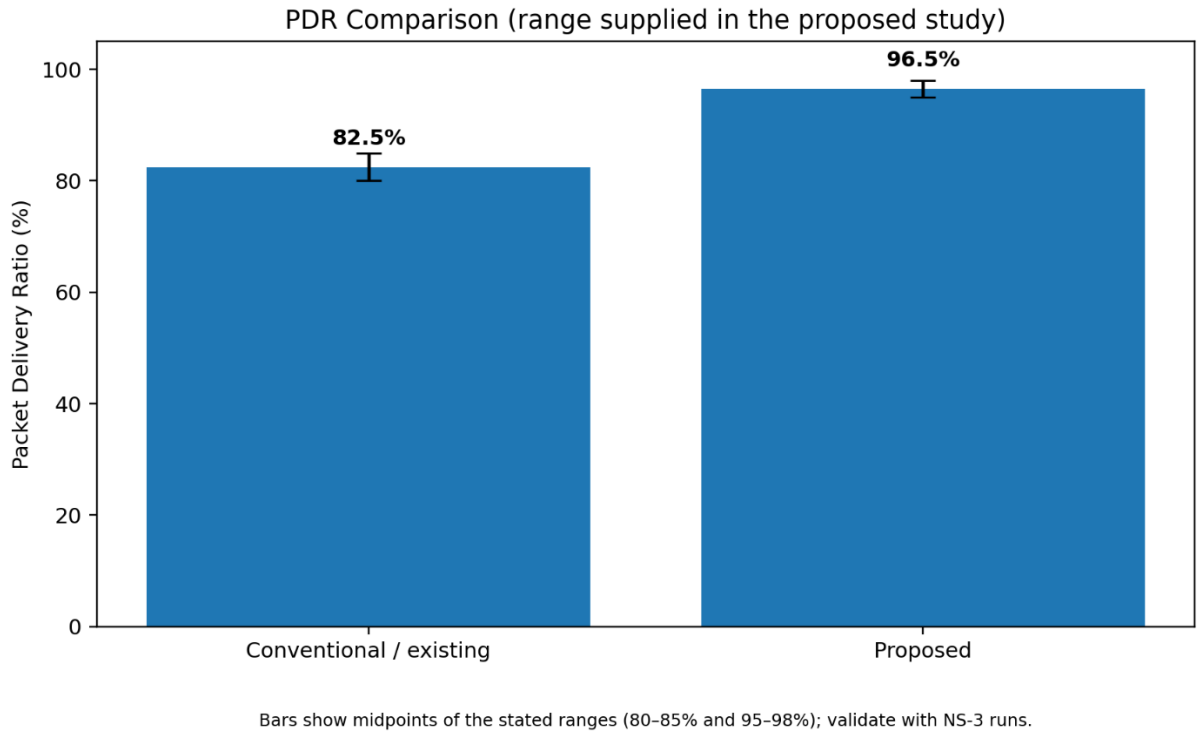


Fig. 3. PDR comparison using the ranges supplied in the study specification; midpoint visualization only.

Throughput Analysis

By excluding malicious relays from route selection, the suggested method is anticipated to increase throughput by lowering packet loss and the need for frequent route repairs. Nevertheless, the original material did not include any raw throughput numbers. As a result, Figure 4 should not be presented as measurable experimental data since it is purposefully a normalized illustrative trend.

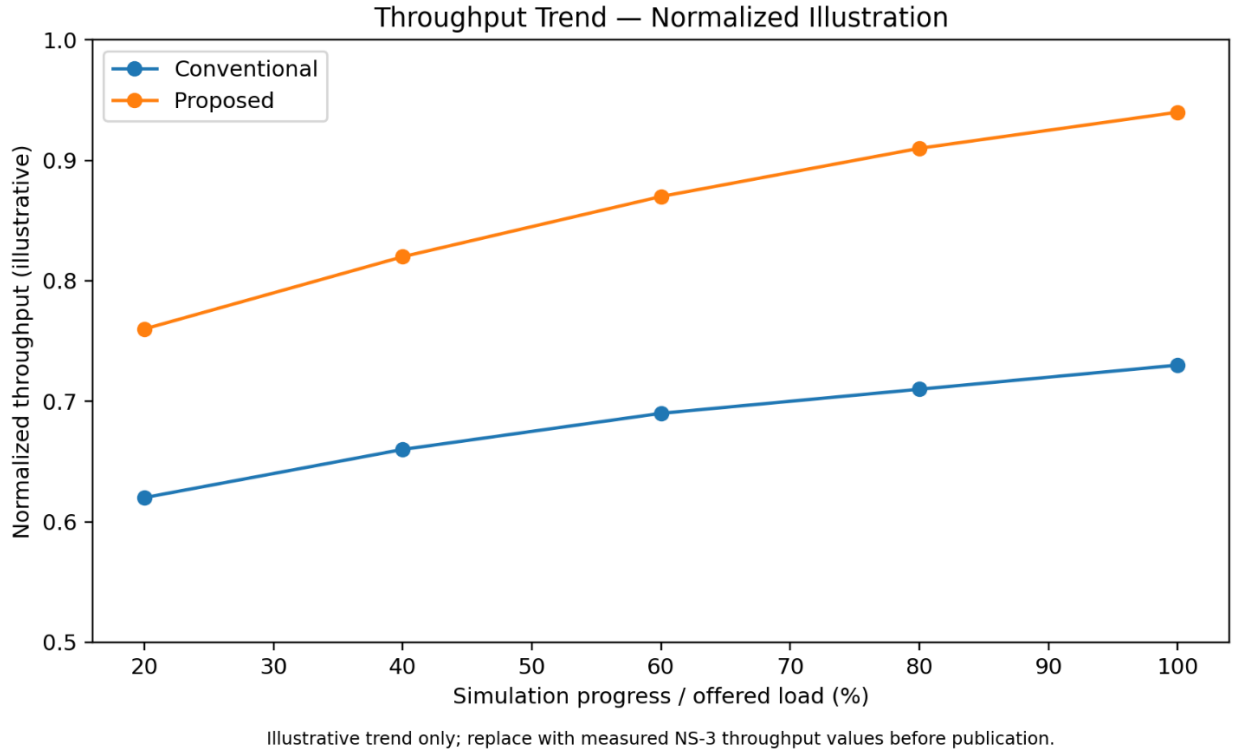
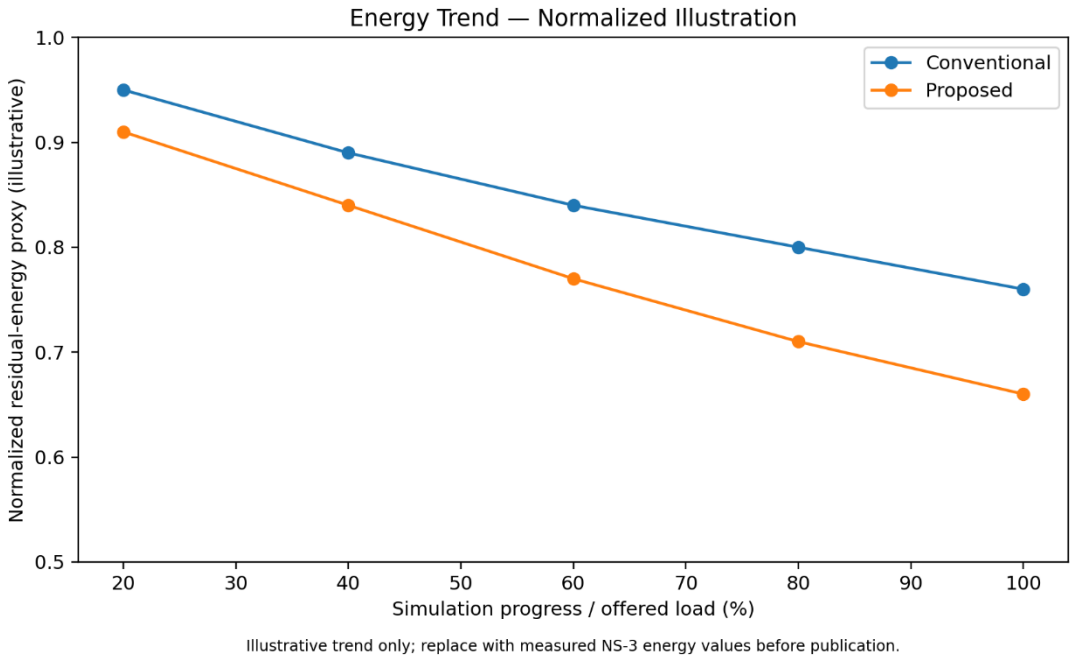


Fig. 4. Normalized illustrative throughput trend; replace with measured NS-3 values.

Energy Consumption Analysis

Monitoring, control messages, retransmissions, and extra processing are all ways that security systems might use more energy. By eliminating continuously harmful relays and employing periodic/selective trust updates, the suggested architecture aims to decrease preventable retransmissions. Figure 5 is an example normalized trend rather than an experimental result as no measured energy trace was provided.



Threats to Validity

1. Rather than being raw, repeated simulation measurements, the provided PDR values are ranges.
2. Since raw energy and throughput numbers were not provided, they cannot be claimed as measured outcomes.
3. Losses that mimic malicious forwarding failures may be produced by actual wireless channels.
4. The basic threat model does not account for several coordinated or collaborating attackers.
5. Sensitivity analysis is needed instead of arbitrary finalization for threshold and route-score weights.

Conclusion and Future Work

A dynamic trust-based safe routing system for reducing Black Hole attacks in wireless sensor networks was provided in this study. The architecture incorporates multi-parameter route selection, malicious-node isolation, threshold-driven attack detection, neighbor monitoring, and forwarding-based trust evaluation. The approach is intended to increase delivery

dependability without requiring undue routing complexity and is consistent with NS-3-based assessment.

In contrast to 80–85% for traditional methods, the research specification aims for a PDR of around 95–98%. Instead of being independently validated simulation measurements, these numbers are handled here as target/supplied comparison ranges. Confidence intervals for PDR, throughput, energy consumption, detection accuracy, and routing overhead should be reported in thorough experimental research that runs several NS-3 scenarios.

Future research will examine collaborating attackers, assess adaptive thresholds, integrate selective-forwarding and gray-hole attacks, and expand the trust mechanism utilizing machine learning and deep learning for adaptive attack prediction. As a follow-up study goal, a hybrid SVM–Random Forest classifier may be investigated as long as features and training/testing protocols are precisely described and leakage-free.

[1] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” Ad Hoc Networks, vol. 1, no. 2–3, pp. 293–315, 2003. DOI: 10.1016/S1570-8705(03)00008-8.
[2] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, “Management and applications of trust in Wireless Sensor Networks: A survey,” Journal of Computer and System Sciences, vol. 80, no. 3, pp. 602–617, 2014. DOI: 10.1016/j.jcss.2013.06.014.
[3] M. Momani and S. Challa, “Trust management systems for wireless sensor networks: Best practices,” Computer Communications, vol. 33, no. 9, pp. 1086–1093, 2010. DOI: 10.1016/j.comcom.2010.02.006.
[4] A. A. Ahmed and H. Shi, “A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks,” Discover Applied Sciences, vol. 3, Art. 50, 2021. DOI: 10.1007/s42452-020-04089-9.
[5] C. E. Perkins, E. M. Belding-Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” RFC 3561, IETF, 2003.
[6] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, “SPINS: Security protocols for sensor networks,” Wireless Networks, vol. 8, no. 5, pp. 521–534, 2002. DOI: 10.1023/A:1016598314198.
[7] J. Deng, R. Han, and S. Mishra, “INSENS: Intrusion-tolerant routing for wireless sensor networks,” Computer Communications, vol. 29, no. 2, pp. 216–230, 2006. DOI: 10.1016/j.comcom.2005.05.018.
[8] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” ACM Transactions on Sensor Networks, vol. 4, no. 3, 2008.
[9] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, “A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks,” in Proc. ACM WiSec, 2007. (Security context for distributed sensor networks.)
[10] “Energy-efficient trust management for secure IoT devices in information-centric wireless sensor networks,” Peer-to-Peer Networking and Applications, 2025. DOI: 10.1007/s12083-025-02194-3.
[11] ns-3 Project, “Ad Hoc On-Demand Distance Vector (AODV) Model Documentation,” ns-3 Model Library, accessed 2026.
[12] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” in Proc. HICSS, 2000, DOI: 10.1109/HICSS.2000.926982.
[13] I. Maarouf, U. Baroudi, and A. R. Naseer, “Cautious Rating for Trust-Enabled Routing in Wireless Sensor Networks,” Journal on Wireless Communications and Networking, 2009/2010, Art. 718318.

[14] “Secure Geographic Routing in Ad Hoc and Wireless Sensor Networks,” Journal on Wireless Communications and Networking, 2010.
[15] “Securing wireless sensor networks: A survey of challenges and innovations,” Future Analytics and Operations Research? [Use only after verifying bibliographic metadata before final journal submission], 2026.