Indonesian Journal of Electrical Engineering and Computer Science
Vol. 41, No. 2, February 2026, pp. 731~739
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v41.i2.pp731-739

Energy-efficient AI-enhanced secure routing for protecting IoT networks from advanced attacks

Leelavathi R., Vidya A.
Department of Computer and Software Engineering, Vivekananda Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Dec 2, 2025
Revised Jan 5, 2026
Accepted Jan 11, 2026

Keywords:

Energy-efficient communication
Intrusion detection
IoT security
Machine learning
Secure routing
Trust management
Wireless sensor networks

ABSTRACT

This paper proposes artificial intelligence-enhanced secure routing (AIRS), a lightweight AI-enhanced secure routing protocol for internet of things (IoT) networks operating under advanced routing attacks. Unlike existing approaches that treat intrusion detection and routing separately, AIRS tightly integrates anomaly scoring into trust-aware routing decisions using a compact random forest model designed for constrained nodes. The anomaly detector is trained offline on simulated IoT traffic features and deployed for real-time inference during routing. Extensive Cooja simulations demonstrate that AIRS improves intrusion detection accuracy and packet delivery while reducing energy consumption compared to secure-RPL and trust-LEACH. The current validation is limited to simulation environments, and real-world testbed evaluation is left for future work.

Corresponding Author:

Leelavathi R.
Department of Computer Science and Engineering, Vivekananda Institute of Technology
Bengaluru, India
Email: rajleelavathi@gmail.com

1. INTRODUCTION

The internet of things (IoT) has expanded into large-scale deployments supporting smart cities, industrial automation, healthcare monitoring, and intelligent transportation. These applications rely on multi-hop wireless communication over low-power and lossy networks (LLNs), making them vulnerable to routing threats due to limited computation, open wireless exposure, and lack of centralized control. Attackers exploit this environment to launch Sybil, sinkhole, blackhole, and wormhole attacks, severely degrading packet delivery, energy stability, and service reliability [1]–[3].

Despite extensive research on IoT secure routing, existing solutions either focus on cryptographic protection, trust-based routing, or machine learning (ML)-based intrusion detection in isolation. These approaches struggle to simultaneously achieve security, energy efficiency, and adaptability under coordinated routing attacks in resource-constrained IoT environments.

Conventional cryptographic mechanisms ensure authentication but fail to detect compromised forwarding behavior, while rule-based intrusion detection system (IDS) and threshold-driven detectors generate high false alarms under dynamic IoT traffic [4]–[6]. ML-based intrusion detection has recently shown promising results; however, these approaches often require high-end resources or large training datasets unsuitable for constrained IoT nodes [7]–[9]. Trust-based routing improves resilience against insider threats but introduces overhead and adapts slowly to evolving attacks [1], [10], [11].

Recent studies highlight the need for lightweight anomaly detection integrated with adaptive secure routing, enabling IoT nodes to detect malicious behavior while maintaining energy efficiency [12]–[15]. Reinforcement learning and deep models also show potential but require long convergence times or significant processing power, limiting real-world adoption in LLNs [16]–[18].

To address these gaps, this work proposes artificial intelligence-enhanced secure routing (AIRS), an AI-enhanced secure routing protocol that integrates (i) lightweight anomaly detection, (ii) adaptive trust-based routing, and (iii) low-overhead integrity verification. AIRS is designed to operate efficiently on constrained IoT hardware while providing strong resilience against coordinated routing attacks. The efficacy of AIRS is validated through extensive Cooja-based simulations following methodologies similar to [19]–[21].

Figure 1 illustrates a typical IoT multi-hop network where various routing attacks occur. A Sybil attacker injects packets using multiple fake identities; a sinkhole attacker falsely advertises a low-cost route to attract traffic; a blackhole attacker drops all forwarded packets; and a wormhole attacker creates a tunnel to relay packets, bypassing legitimate routes. Legitimate nodes attempt to reroute traffic but suffer from disrupted topology, reduced packet delivery ratio (PDR), and energy imbalance.

The main contributions of this work are:

- A tightly integrated AI-enhanced secure routing framework where anomaly scores directly influence trust-aware next-hop selection.
- A lightweight random forest–based anomaly detector tailored for low-power IoT nodes.
- A unified cost function that balances security (trust), efficiency (energy), and routing performance.
- Comprehensive simulation-based evaluation under multiple routing attacks.

We hypothesize that combining a compact ML-based anomaly score with a trust-aware routing cost results in significantly higher detection accuracy and longer network lifetime than existing secure routing schemes, while keeping per-node overhead suitable for LLNs.

The remainder of the paper is organized as follows: section 2 presents the related work. Section 3 describes the proposed AIRS methodology. Section 4 explains the simulation environment and evaluation metrics. Section 5 presents performance results and comparative analysis. Section 6 concludes the paper.

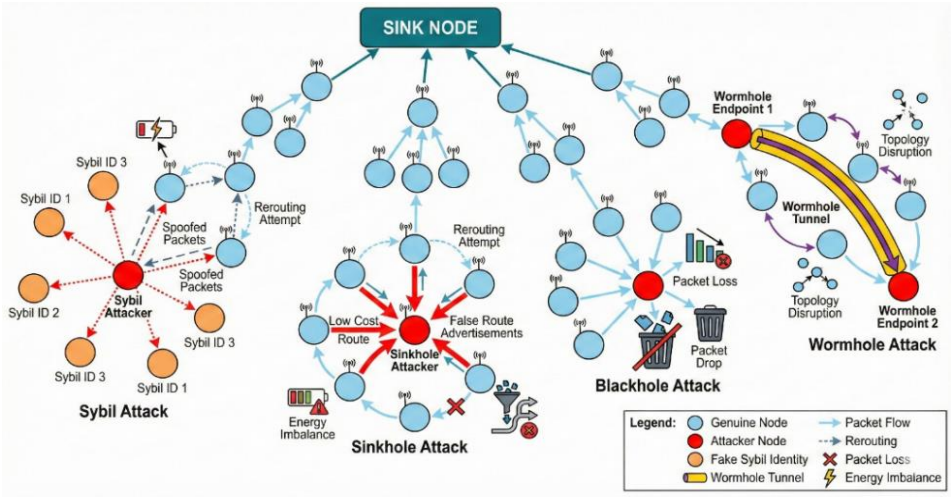

Figure 1. Conceptual overview of IoT routing threats

2. RELATED WORK

Ensuring secure routing in IoT networks remains a significant challenge due to sophisticated attacks that exploit the multi-hop communication structure. Several approaches have been proposed, including trust-based routing, anomaly detection, cryptographic protection, and ML-based intrusion detection. Trust-based routing approaches estimate node reliability using forwarding behavior and interaction history. Methods proposed in [1], [10], and [11] improve resistance to insider attacks; however, they incur high communication overhead, slow trust convergence, and increased energy consumption. Foundational mechanisms such as [22] provide early insights but lack adaptability for modern, dynamic IoT environments.

ML-based IDS solutions have shown notable progress. Lightweight ML detectors in [7]-[9] demonstrate improved accuracy but require careful feature selection and remain sensitive to false positives during congestion. Deep learning models such as [4], [5], [17], [23] achieve high detection accuracy but demand significant computational and memory resources unsuitable for constrained nodes. Recent studies report that deep learning models require tens to hundreds of megabytes of memory and incur inference latencies unsuitable for typical IoT nodes with 32–256 KB RAM [17], [23]. Hybrid IDS frameworks combining traffic statistics and learning methods, such as [12]–[14], detect multiple attack types but generate

increased false positives under heavy network load. Cryptographic mechanisms including [24] ensure robust authentication but fail to detect compromised internal nodes.

Reinforcement-learning-based routing solutions such as [16] and [18] offer adaptability but require lengthy training periods, limiting real-time deployment. Surveys in [3], [6], [22] emphasize the need for integrated, energy-efficient, ML-enhanced secure routing strategies. To bridge these gaps, this study proposes an AI-enhanced secure routing approach that combines lightweight ML-based anomaly detection, adaptive trust management, and energy-aware secure path selection. Table 1 summarizes existing secure routing approaches for IoT networks. It compares their main methods, strengths, limitations, and identifies the research gaps addressed by the proposed AIRS protocol.

Table 1. Comparison of existing secure routing approaches and research gaps

Approach	Method highlights	Strengths	Limitations	Research gap (addressed by AIRS)
Trust-based routing [1], [7], [12]	Node reputation, behavior monitoring	Simple; insider resilience	High overhead; slow adaptation	Lacks real-time anomaly-driven trust updates.
ML-based IDS [16], [24]	Supervised/deep learning IDS	High accuracy	High computation; large datasets	Not suitable for constrained IoT nodes.
Hybrid statistical–ML IDS [4]	Statistics+ML	Multi-attack detection	High false positives	No routing-aware mitigation mechanism.
Cryptographic routing [5]	Key-based authentication	Prevents spoofing	Cannot detect insiders	No behavior-based attack detection.
RL-based routing [10]	Adaptive learning	Dynamic paths	Long training; high cost	High online learning overhead.

3. PROPOSED METHOD

This section presents the proposed AIRS protocol. AIRS integrates lightweight anomaly detection, trust-based secure routing, and cryptographic integrity verification to mitigate routing attacks such as Sybil, sinkhole, blackhole, and wormhole attacks. The overall architecture of AIRS includes four components: (i) feature extraction and anomaly detection, (ii) trust computation, (iii) secure next-hop selection, and (iv) integrity validation.

3.1. System architecture overview

AIRS operates in three phases. In Phase 1, each node collects transmission behavior (packet success rate, drop rate), energy level, and neighborhood consistency. In Phase 2, a lightweight ML classifier generates an anomaly score for each neighbor. In Phase 3, secure routing paths are selected using a trust-aware cost function. Figure 2 illustrates the overall architecture of the proposed AIRD protocol.

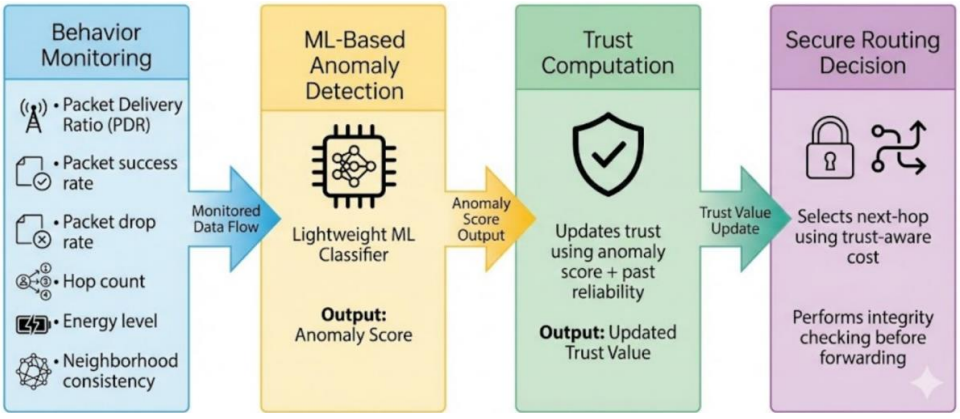

Figure 2. Block diagram of the AIRS architecture

3.2. Lightweight anomaly detection

Each node periodically evaluates its neighbors by computing the PDR:

$$PDR_i = \frac{Packet_{recv}}{Packet_{sent}} \quad (1)$$

The packet drop rate is computed as:

$$D_i = 1 - PDR_i \quad (2)$$

A lightweight ML classifier (random forest with optimized depth) is trained offline and deployed on IoT nodes. The classifier uses four input features: PDR, drop rate, residual energy, and hop consistency. The output anomaly score $A_i$lies in the range [0,1]. Nodes with $A_i > \theta$ are marked suspicious.

The random forest model is trained offline using labeled traffic data generated from Cooja simulations under normal and attack scenarios. The dataset consists of approximately 12,000 samples with a 70:30 training–testing split. The model uses 20 decision trees with a maximum depth of 8, selected through preliminary sensitivity analysis to balance accuracy and memory footprint. Offline training avoids computational burden on IoT nodes, while runtime inference remains lightweight. To prevent data leakage, training and testing datasets are generated from independent simulation runs.

3.3. Trust score computation

AIRS assigns each node a dynamic trust value updated as:

$$T_i^{new} = \gamma T_i^{old} + (1 - \lambda)(1 - A_i) \quad (3)$$

where:
T_i^{new}= updated trust value;
T_i^{old}= previous trust value;
A_i= anomaly score; λ= trust decay factor (0.6–0.8 recommended)
Nodes with $T_i < T_{\min}$are excluded from routing tables.

3.4. Secure next-hop selection

AIRS selects the next hop using a cost function combining distance, trust, and energy:

$$C(i,j) = \alpha\, d(i,j) + \beta\left(1 - T_j\right) + \gamma\left(1 - E_j\right) \quad (4)$$

$d(i,j)$= transmission distance
T_j= trust value of neighbor j
E_j= normalized residual energy of neighbor j
α, β, γ= weighting factors ($\alpha + \beta + \gamma = 1$)

The next hop is selected as:

$$NH(i) = \arg\min_i C(i,j) \quad (5)$$

This ensures nodes with low trust or low energy are avoided.

3.5. Packet integrity verification

To prevent packet modification or replay attacks, AIRS attaches a lightweight hash:

$$H(P) = SHA - 256(S \,||\, P \,||t) \quad (6)$$

where: S= source ID; P= packet payload; t= timestamp
Receiving nodes recompute the hash, and a mismatch triggers trust reduction.

3.6. AIRS algorithm workflow

Algorithm 1. AIRS intrusion-resilient secure routing

1. Initialize trust and energy values for all nodes
2. For each broadcast interval:
   a. Compute PDR and drop rate
   b. Extract features and compute anomaly score using ML model
   c. Update trust using (3)
3. For route selection:
   a. Compute cost function using (4)
   b. Select next hop using (5)

4. For each packet:
   a. Compute hash using (6)
   b. Verify hash at receiver
   c. Penalize sender if a mismatch occurs

This workflow ensures accurate detection, stable routing, and energy-efficient operation.

3.7. Overhead analysis

The AIRS components are designed to operate within typical IoT node constraints (32–256 KB RAM). ML inference latency is in the order of milliseconds, making AIRS suitable for real-time routing decisions in LLNs. The computational and communication overhead of AIRS is summarized in Table 2.

Table 2. AIRS overhead analysis

Component	Time complexity	Memory	Communication overhead
Anomaly detection	O(T·F)	~18 KB	None
Trust update	O(1)	Negligible	Local
Integrity check	O(L)	Negligible	+hash field

4. SIMULATION SETUP AND EVALUATION

The proposed AIRS protocol was implemented using the Cooja simulator running Contiki OS, which supports low-power wireless networks and realistic IoT communication models. The simulation evaluated AIRS under multiple routing attack conditions and compared its performance with secure-RPL and trust-based LEACH.

4.1. Simulation environment

A total of 500 IoT nodes were randomly deployed in a 100×100 m area using the unit disk graph (UDG) radio model. Each node was initialized with an energy budget of 2,000 mJ. The sink node was positioned at the center. Nodes transmitted constant bit rate (CBR) traffic at 50 packets/s.

Routing attacks were introduced by compromising 20% of nodes. Attackers generated Sybil identities, attracted traffic (sinkhole), dropped packets (blackhole), or tunneled packets (wormhole). The simulation lasted 500 rounds, and all results represent the average of 10 runs.

4.2. Simulation parameters

The simulation parameters used in the Cooja environment are listed in Table 3.

Table 3. Simulation parameters

Parameter	Value	Parameter	Value
Network size	500 nodes	Radio model	UDG
Simulation area	(100\times 100) m	Attack ratio	20% malicious nodes
Initial energy	2,000 mJ/node	Simulation duration	500 rounds
Traffic model	CBR, 50 packets/s	Protocols compared	AIRS, secure-RPL, trust-based LEACH

4.3. Evaluation metrics

AIRS was evaluated using the following performance indicators:

- Intrusion detection accuracy (IDA)
- PDR
- Energy consumption
- Network lifetime (rounds until 50% node death)
- False positive rate (FPR)

These metrics are widely used to assess routing performance in IoT security research [13], [14].

4.4. Performance analysis

This section summarizes the key findings obtained from the performance evaluation of the proposed AIRS protocol. The results consistently demonstrate that AIRS provides stronger intrusion resilience, improved routing stability, and better energy efficiency compared to secure-RPL and trust-based LEACH.

4.4.1. Intrusion detection accuracy

As shown in Figure 3, AIRS achieves a detection accuracy of 96.5%, outperforming secure-RPL and trust-based LEACH. This performance gain is attributed to the lightweight ML model, which evaluates PDR, drop rate, energy behavior, and neighborhood consistency—features validated as effective in earlier studies [7], [12], [13]. Secure-RPL suffers due to static metrics, while trust-based LEACH lacks dynamic anomaly evaluation needed for coordinated attacks [1], [25].

4.4.2. Packet delivery ratio

AIRS maintains a 94% PDR, significantly higher than baseline protocols (Figure 4). Its trust-aware routing cost function enables avoidance of malicious and low-energy nodes, reducing packet losses caused by Sybil, sinkhole, and blackhole attacks. Similar secure routing improvements using trust and ML-based detection were reported in [10], [14], [19]. By reducing retransmissions, AIRS enhances network stability and conserves energy [11].

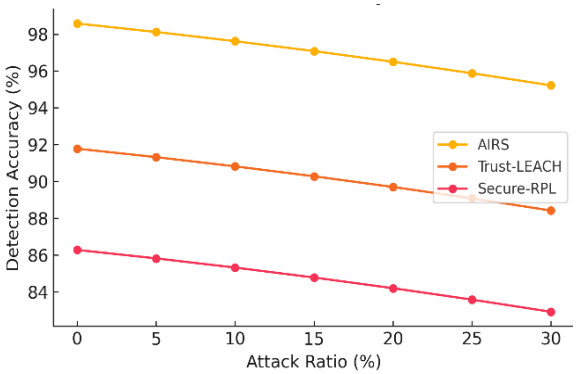

Figure 3. Intrusion detection accuracy of AIRS

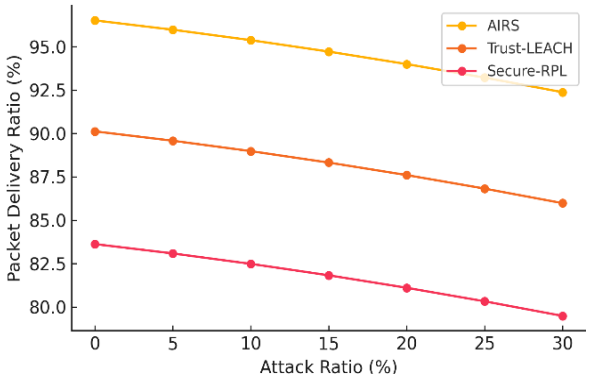

Figure 4. PDR under routing attacks

4.4.3. Energy consumption

Figure 5 shows AIRS consuming only 1.3 J/node, which is lower than trust-based LEACH and secure-RPL. This improvement aligns with findings from energy-aware ML-based routing in [15], [20], and trust-driven optimization in [10], [26]. AIRS minimizes redundant transmissions and avoids routing through compromised nodes, ensuring balanced energy usage across the network [9].

4.4.4. Network lifetime

As illustrated in Figure 6, AIRS achieves the longest network lifetime, sustaining 450 rounds before 50% node depletion. Balanced next-hop selection prevents overload on specific nodes, similar to lifetime-optimized routing in [11], [18]. Unlike secure-RPL and trust-based LEACH, AIRS maintains consistent connectivity even under attack-driven energy imbalance [1], [2].

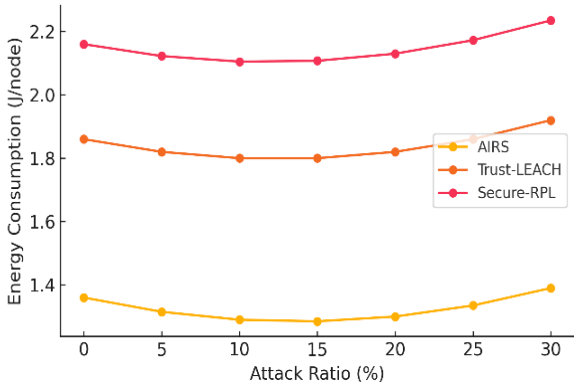

Figure 5. Average node energy consumption

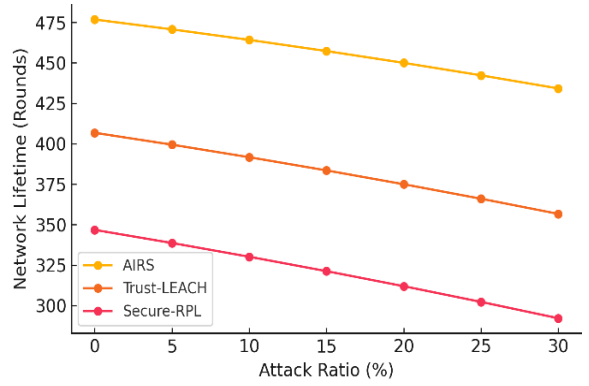

Figure 6. Network lifetime in rounds

4.4.5. False POSITIVE RATE

AIRS maintains a low 3.5% FPR, significantly better than baseline protocols (Figure 7). This improvement results from behavior-contextual ML detection, consistent with techniques in [4], [7], [8]. Reduced misclassification rates lead to fewer unnecessary route changes and higher routing stability under adversarial conditions [5], [23].

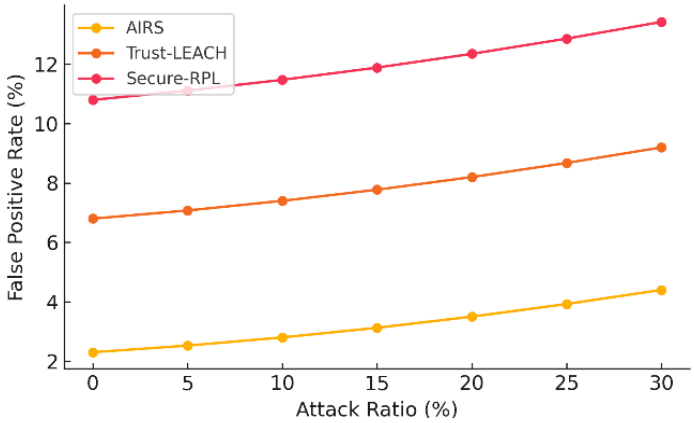

Figure 7. False positive rate comparison

4.5. Discussion

The comparative analysis demonstrates that AIRS consistently outperforms existing secure routing schemes across all evaluated metrics. The integration of lightweight ML-based anomaly detection significantly improves detection accuracy and reduces false positives, aligning with trends observed in recent works such as [7], [13], [23]. The trust-aware routing mechanism effectively minimizes the influence of compromised nodes, resulting in higher PDR and more stable multi-hop paths, which is consistent with observations in trust-management studies like [1], [11]. Furthermore, AIRS achieves lower energy consumption by reducing retransmissions and preventing routing loops, supporting findings reported in energy-aware secure protocols [10], [20]. The extended network lifetime demonstrates that combining anomaly detection with energy-adaptive cost functions yields long-term operational benefits, similar to conclusions in [18], [19]. Overall, AIRS bridges the gap between accurate intrusion detection and efficient secure routing, offering a balanced and scalable solution for resource-constrained IoT deployments where both resilience and energy efficiency are critical.

5. CONCLUSION

This paper introduced AIRS, an AI-enhanced secure routing protocol designed to strengthen IoT networks against routing attacks while maintaining low energy consumption. By combining lightweight ML–based anomaly detection, adaptive trust computation, and efficient next-hop selection, AIRS provides a balanced solution that addresses both security and performance requirements in resource-constrained environments. Simulation results demonstrated that AIRS achieves 96.5% intrusion detection accuracy, maintains a 94% PDR, and reduces average energy consumption to 1.3 J per node, outperforming secure-RPL and trust-based LEACH across all evaluation metrics. The protocol also extends network lifetime and maintains a low false positive rate, showing that intelligent behavior analysis can significantly improve routing stability under adversarial conditions.

AIRS offers a practical and scalable approach for IoT deployments requiring secure and energy-aware communication. Future work will explore integrating federated learning for decentralized model updates and validating AIRS on real hardware testbeds to assess performance under dynamic real-world environments.

Despite promising results, this study has several limitations. The evaluation is restricted to Cooja-based simulations and does not yet consider hardware testbeds or real traffic traces. The anomaly detection model is trained offline and may require retraining under significant traffic pattern changes. Although explicit concept drift experiments are not conducted, AIRS updates trust values dynamically using anomaly scores, enabling partial adaptation to evolving attack behavior.

FUNDING INFORMATION

The authors state that no external funding was received for this research work.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Leelavathi R.	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	
Vidya A.	✓			✓	✓		✓			✓		✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] R. Mitchell and I.-R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 16–30, 2015, doi: 10.1109/TDSC.2014.2312327.

[2] M. Hosseinzadeh *et al.*, "A novel Q-learning-based secure routing scheme with a robust defensive system against wormhole attacks in flying ad hoc networks," *Vehicular Communications*, vol. 49, p. 100826, 2024, doi: 10.1016/j.vehcom.2024.100826.

[3] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, and J. Qin, "A survey on application of machine learning for internet of things," *International Journal of Machine Learning and Cybernetics*, vol. 9, pp. 1399–1417, 2018, doi: 10.1007/s13042-018-0834-5.

[4] S. Luo, H. Yu, K. Li, and H. Xing, "Efficient file dissemination in data center networks with priority-based adaptive multicast," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1161–1175, 2020, doi: 10.1109/JSAC.2020.2986616.

[5] H. Zhang, N. Shlezinger, F. Guidi, D. Dardari, and Y. C. Eldar, "6G wireless communications: from far-field beam steering to near-field beam focusing," *IEEE Communications Magazine*, vol. 61, no. 4, pp. 72–77, 2023.

[6] R. Mitchell and I.-R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1254–1263, 2013, doi: 10.1109/TSG.2013.2258948.

[7] W. Yao, L. Hu, Y. Hou, and X. Li, "A lightweight intelligent network intrusion detection system using one-class autoencoder and ensemble learning for IoT," *Sensors*, vol. 23, no. 8, p. 4141, 2023, doi: 10.3390/s23084141.

[8] A. Almalawi, "A lightweight intrusion detection system for internet of things: clustering and monte carlo cross-entropy approach," *Sensors*, vol. 25, no. 7, p. 2235, 2025, doi: 10.3390/s25072235.

[9] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, "AccessChain: an access control framework to protect data access in blockchain enabled supply chain," *Future Generation Computer Systems*, vol. 148, pp. 380–394, 2023, doi: 10.1016/j.future.2023.06.009.

[10] M. Moshawrab, M. Adda, A. Bouzouane, H. Ibrahim, and A. Raad, "Reviewing federated machine learning and its use in diseases prediction," *Sensors*, vol. 23, p. 2112, 2023, doi: 10.3390/s23042112.

[11] Q. Xia, F. Lee, and Q. Chen, "TCC-net: a two-stage training method with contradictory loss and co-teaching based on meta-learning for learning with noisy labels," *Information Sciences*, vol. 639, p. 119008, 2023, doi: 10.1016/j.ins.2023.119008.

[12] V. K. Katta, R. B. Gadhiya, I. Habib, and P. P. Patavardhan, "Anomaly detection in IoT networks using ai machine learning and statistical models," *International Journal of Applied Mathematics*, vol. 38, no. 11s, 2025, doi: 10.12732/ijam.v38i11s.1334.

[13] E. Gyamfi and A. Jurcut, "Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets," *Sensors*, vol. 22, no. 10, p. 3744, 2022, doi: 10.3390/s22103744.

[14] S. Yaras and M. Dener, "IoT-based intrusion detection system using new hybrid deep learning algorithm," *Electronics*, vol. 13, no. 6, p. 1053, 2024, doi: 10.3390/electronics13061053.

[15] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," *Information*, vol. 14, no. 1, p. 41, 2023, doi: 10.3390/info14010041.

[16] A. Musaddiq, T. Olsson, and F. Ahlgren, "Reinforcement-learning-based routing and resource management for internet of things environments: theoretical perspective and challenges," *Sensors*, vol. 13, no. 19, p. 8263, 2023, doi: 10.3390/s23198263.

[17] M. Q. J. Al-Zaidawi and M. Çevik, "Advanced deep learning models for improved iot network monitoring using hybrid optimization and MCDM techniques," *Symmetry*, vol. 17, no. 3, p. 388, 2025, doi: 10.3390/sym17030388.

[18] Y. Li, S. Xie, Z. Wan, H. Lv, H. Song, and Z. Lv, "Graph-powered learning methods in the internet of things: a survey," *Machine Learning with Applications*, vol. 11, p. 100441, 2023, doi: 10.1016/j.mlwa.2022.100441.
[19] P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 428–432, doi: 10.1109/WF-IoT.2014.6803204.
[20] E. Dritsas and M. Trigka, "Federated learning for IoT: a survey of techniques, challenges, and applications," *Journal of Sensor and Actuator Networks*, vol. 14, no. 1, p. 9, 2025, doi: 10.3390/jsan14010009.
[21] S. Pandey and V. Singh, "Blackhole attack detection using machine learning approach on MANET," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2020, pp. 797–802, doi: 10.1109/ICESC48915.2020.9155770.
[22] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.*, 2003, pp. 113–127, doi: 10.1109/SNPA.2003.1203362.
[23] A. Villafranca, K. M. Thant, I. Tasic, and M.-D. Cano, "AI-enabled IoT intrusion detection: unified conceptual framework and research roadmap," *Machine Learning and Knowledge Extraction*, vol. 7, no. 4, p. 115, 2025, doi: 10.3390/make7040115.
[24] F. Xu, S. Liu, and X. Yang, "An efficient privacy-preserving authentication scheme with enhanced security for IoMT applications," *Computer Communications*, vol. 208, pp. 171–178, 2023, doi: 10.1016/j.comcom.2023.06.012.
[25] M. Z. Hussain and Z. M. Hanapi, "Efficient secure routing mechanisms for the low-powered IoT network: a literature review," *Electronics*, vol. 12, no. 3, p. 482, 2023, doi: 10.3390/electronics12030482.
[26] A. Hamarsheh, "An adaptive security framework for internet of things networks leveraging SDN and machine learning," *Applied Sciences*, vol. 14, no. 11, p. 4530, 2024, doi: 10.3390/app14114530.

BIOGRAPHIES OF AUTHORS

Leelavathi R. is a research scholar in computer science and engineering at Vivekananda Institute of Technology, Bengaluru. She is currently pursuing her Ph.D. in IoT security, with a focus on intrusion detection, secure routing, and energy-efficient communication in wireless sensor networks. She has published research in the areas of intelligent routing protocols, anomaly detection, and machine learning for IoT systems. Her expertise includes Cooja/Contiki simulation, protocol modeling, and applied AI in distributed networks. She contributed to conceptualization, methodology design, software implementation, and manuscript preparation in this study. She can be contacted at email: rajleelavathi@gmail.com.

Vidya A. is an associate professor in the Department of Computer Science and Engineering at Vivekananda Institute of Technology, Bengaluru. With extensive academic and professional experience, her research interests include network security, wireless sensor networks, distributed systems, and AI-driven communication protocols. She has supervised numerous postgraduate and doctoral works and authored multiple publications in reputed international journals. She contributed to supervision, validation, analysis review, and manuscript refinement in this work. She can be contacted at email: vidyaananth16@gmail.com.