International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 15, No. 3, November 2026, pp. 868~877
ISSN: 2089-4864, DOI: 10.11591/ijres.v15.i3.pp 868-877

Multi-metric trust-based secure routing with intelligent anomaly detection for robust IoT network communication

Sangeetha Krishnaswamy[1], Arulanandam Karalagan[2]
[1]Department of Computer Science and Applications, Adhiparasakthi College of Arts and Science (Autonomous), (Affiliated to Thiruvalluvar University, Vellore), Kalavai, India
[2]Department of Computer Science, Government Thirumagal Mills College, Gudiyattam, India

Article Info

Article history:

Received Mar 10, 2026
Revised Aug 13, 2026
Accepted Sep 11, 2026

Keywords:

Biomedical news
Convolutional neural network
Detection
Graph neural network
Machine learning

ABSTRACT

The rapid expansion of the internet of things (IoT) has introduced significant challenges in ensuring secure, reliable, and energy-efficient communication across heterogeneous networks. This paper proposes a multi-metric trust-based secure routing (MMTSR) framework that combines comprehensive trust evaluation with intelligent anomaly detection to mitigate routing attacks and enhance overall network performance. The trust evaluation model aggregates multiple behavioral and performance metrics, including packet forwarding ratio (PFR), residual energy (RE), packet loss rate (PLR), communication delay (CD), and historical interaction reliability (HIR), to compute a composite trust score for each node. Simultaneously, a machine learning-based anomaly detection module identifies malicious nodes based on traffic behavior, routing updates, and packet transmission patterns. Simulation results demonstrate that MMTSR significantly outperforms conventional routing protocols, achieving a packet delivery ratio of 97.8%, average throughput of 470 kbps, and end-to-end delay of 46 ms under a 10% malicious node scenario, while reducing routing overhead and energy consumption to 150 packets and 0.95 J per node, respectively. The anomaly detection module achieves a detection accuracy of 97.6% with a false positive rate of only 2.5%, effectively identifying blackhole, selective forwarding, Sybil, and packet dropping attacks. Comparative analysis with recent studies further confirms the framework's superiority in terms of reliability, security, and efficiency.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Sangeetha Krishnaswamy
Department of Computer Science and Applications
Adhiparasakthi College of Arts and Science (Autonomous)
(Affiliated to Thiruvalluvar university, Vellore)
Kalavai, Ranipet, Tamil Nadu, India
Email: sangeetha19892005@gmail.com

1. INTRODUCTION

The rapid expansion of the internet of things (IoT) has transformed the landscape of modern digital infrastructure by enabling seamless connectivity among a wide range of smart devices, sensors, and embedded systems. IoT networks have become fundamental components in numerous domains such as smart healthcare, intelligent transportation, environmental monitoring, industrial automation, and smart city applications. In these environments, thousands or even millions of heterogeneous devices interact continuously to collect, process, and transmit data. While this interconnected ecosystem enhances operational efficiency and real-time decision making, it also introduces substantial challenges related to communication reliability, network scalability, and security [1]-[4]. Unlike traditional networks, IoT devices are often resource-constrained,

possessing limited computational power, storage capacity, and energy resources. These constraints make the design of efficient and secure communication protocols significantly more complex. Additionally, IoT deployments frequently operate in highly dynamic environments where nodes may join or leave the network unpredictably, network topologies change frequently, and communication links are often unreliable. As a result, ensuring reliable data transmission while maintaining security and performance has become a critical research challenge in IoT network design [5]-[8].

One of the most critical aspects of IoT communication lies in the routing mechanisms that determine how data packets travel from source nodes to destination nodes. In large-scale IoT environments, multi-hop communication is commonly employed because many devices cannot directly communicate with centralized gateways due to limited transmission ranges. Consequently, intermediate nodes play a vital role in forwarding packets across the network. However, this reliance on intermediate nodes introduces significant security vulnerabilities. Malicious or compromised nodes may intentionally disrupt network operations by launching various routing attacks such as packet dropping, route manipulation, sinkhole attacks, or selective forwarding [9]-[12]. These attacks can severely degrade network performance, reduce packet delivery reliability, and compromise the integrity of transmitted data. Traditional routing protocols designed for mobile ad hoc networks (MANETs), such as ad hoc on-demand distance vector, were not originally developed with IoT-specific constraints and security requirements in mind. As a result, they often lack effective mechanisms to evaluate the trustworthiness of participating nodes or detect malicious behaviors during routing operations. When such protocols are directly applied to IoT environments, they become susceptible to insider attacks in which compromised nodes behave normally during route discovery but maliciously during packet forwarding [13]-[15]. Detecting malicious activities becomes particularly challenging in IoT environments where nodes operate autonomously and interactions occur continuously across distributed networks. Furthermore, the constrained nature of IoT devices limits the feasibility of deploying computationally intensive security mechanisms. Therefore, lightweight yet effective security solutions are required to maintain network reliability without imposing excessive resource consumption [16]-[19].

To address these challenges, researchers have increasingly explored trust-based routing (TBR) mechanisms as a promising approach for enhancing IoT network security. TBR introduces the concept of evaluating the reliability of nodes based on their observed behaviors and historical interactions. Instead of blindly relying on routing advertisements, nodes maintain trust values that reflect the credibility of neighboring devices. These trust values are used to guide routing decisions, allowing the network to prioritize communication paths that involve trustworthy nodes while avoiding those that exhibit suspicious or malicious behavior. However, many existing trust-based approaches rely on a limited set of parameters, such as packet forwarding success or simple reputation scores [20]-[22]. While these single-metric trust models offer some level of protection, they may not capture the full complexity of node behavior in dynamic IoT environments [23]-[26]. For example, a node might appear trustworthy based on packet forwarding rates but may still cause performance degradation due to excessive delay, energy depletion, or intermittent malicious actions.

Motivated by these challenges and opportunities, this paper proposes a multi-metric trust-based secure routing (MMTSR) framework with intelligent anomaly detection designed to improve the reliability and security of IoT network communication. The proposed framework evaluates node trustworthiness using multiple metrics that capture both performance characteristics and behavioral patterns.

2. LITERATURE REVIEW

The increasing deployment of the IoT has led to extensive research on secure routing and intrusion detection mechanisms to protect network communication from malicious threats. IoT networks consist of heterogeneous and resource-constrained devices that communicate over dynamic wireless environments, making them highly vulnerable to various routing attacks. To address these challenges, recent studies have focused on integrating intelligent security mechanisms such as trust evaluation, machine learning-based anomaly detection, and software-defined networking (SDN) architectures to improve network reliability and resilience.

Rui *et al.* [11] proposed a secure routing approach for IoT networks that integrates software-defined networking (SDN) with machine learning-based intrusion detection. The proposed framework uses SDN-based network management to monitor communication and identify potential malicious activities. An intelligent detection mechanism analyzes network traffic to recognize attacks and support secure routing decisions. The integration of SDN and machine learning improves network monitoring and adaptive security control. However, dependence on controller-based network management may increase management complexity in large-scale IoT environments.

Subramaniam *et al.* [10] proposed a hybrid intrusion and anomaly detection system for IoT environments that integrates a conditional generative adversarial network (cGAN), slime mould algorithm (SMA), and CNN-LSTM model. The cGAN addresses class imbalance, while SMA is employed for feature

selection to reduce unnecessary features. The CNN-LSTM model captures spatial and temporal characteristics of network traffic for attack detection. The proposed approach achieved improved intrusion detection performance; however, its primary focus is anomaly detection rather than trust-based secure routing.

Trust management has emerged as an important mechanism for enhancing routing security in distributed IoT networks. Gali and Nidumolu [4] proposed an intelligent trust sensing scheme with a metaheuristic-based secure routing protocol for IoT environments. The approach evaluates node trustworthiness and employs metaheuristic optimization to support secure routing decisions. The proposed method improves routing reliability by reducing the participation of untrusted nodes in communication. However, trust evaluation and optimization processes may introduce additional computational overhead in resource-constrained IoT environments.

Li *et al.* [6] proposed an enhanced hybrid particle swarm optimization (EHPSO) algorithm for IoT applications. The method improves the conventional particle swarm optimization process to enhance search capability and optimization performance. The proposed approach demonstrates the usefulness of intelligent optimization techniques for addressing optimization problems associated with IoT environments. However, its main focus is optimization rather than trust evaluation or malicious-node detection, and therefore it does not directly provide a complete trust-based secure routing mechanism.

Venketesh and Sasikala [17] developed an intrusion detection system for MANETs using feature selection and an improved grey wolf optimization-artificial neural network (IGWO-ANN) classification algorithm. The framework performs preprocessing and feature selection before applying the IGWO-ANN classifier to identify malicious network activities. The proposed model improves intrusion detection performance compared with conventional classification approaches. However, the method mainly focuses on intrusion detection and does not fully integrate trust-based routing mechanisms for secure path selection.

To address these limitations, the present study proposes an MMTSR integrated with intelligent anomaly detection mechanisms for robust IoT network communication. The proposed approach evaluates node trustworthiness using multiple behavioral and performance metrics while simultaneously employing machine learning techniques to detect malicious activities. By combining these mechanisms, the framework aims to improve routing reliability, enhance attack resilience, and ensure secure communication in dynamic IoT networks.

3. PROPOSED METHOD

The proposed MMTSR is designed to provide secure and reliable communication in large-scale IoT environments. The architecture integrates trust computation, anomaly detection, and adaptive routing decision mechanisms to mitigate routing attacks and improve overall network performance. The framework operates in a distributed manner, where each node continuously monitors neighboring nodes and updates trust values based on their observed behavior.

3.1. Trust evaluation module

The trust evaluation module is responsible for collecting behavioral and performance information from neighboring nodes. Each node maintains a local trust table that records interactions with neighboring nodes, including packet forwarding behavior, communication delay (CD), and energy status. These observations are periodically updated and used as input parameters for trust computation.

The trust evaluation process begins when nodes monitor packet transmission activities during routing operations. For example, when node n_i sends a packet through node n_j, it observes whether the packet is successfully forwarded. If the packet is forwarded correctly, the trust value associated with n_j increases; otherwise, it decreases. These observations are stored as behavioral metrics and forwarded to the aggregation module.

3.2. Multi-metric trust evaluation model

The core component of the proposed framework is the multi-metric trust evaluation model, which computes the trustworthiness of each node based on multiple behavioral and performance indicators. This approach provides a more comprehensive evaluation compared with traditional single-metric trust models. Let Ti_j represent the trust value assigned by node n_i to its neighboring node n_j. The trust value is calculated using a weighted combination of several trust metrics:

$$T_{ij} = w_1 PFR + w_2 RE + w_3 PLR + w_4 CD + w_5 HIR$$

where, PFR is packet forwarding ratio, RE is residual energy, PLR is packet loss rate, CD is communication delay, HIR is historical interaction reliability, and w_1, w_2, w_3, w_4, w_5 represent weighting coefficients.

The sum of weights satisfies:

$$w_1 + w_2 + w_3 + w_4 + w_5 = 1$$

a. Packet forwarding ratio

PFR measures how reliably a node forwards packets received from neighboring nodes.

$$PFR = \frac{P_{forwarded}}{P_{received}}$$

where $P_{forwarded}$ is the number of packets successfully forwarded and $P_{received}$ is the total number of packets received.

b. Residual energy

RE indicates the remaining energy level of the node relative to its initial energy.

$$RE = \frac{E_{remaining}}{E_{initial}}$$

Nodes with higher RE are more reliable for packet forwarding.

c. Packet loss rate

PLR represents the fraction of packets lost during transmission.

$$PLR = \frac{P_{lost}}{P_{sent}}$$

Lower PLRs indicate higher node reliability.

d. Communication delay

CD measures the time required for a packet to travel from one node to the next.

$$CD = \frac{\sum_{k=1}^{n}(t_{receive} - t_{send})}{n}$$

Lower CDs indicate efficient node performance.

e. Historical interaction reliability

HIR reflects the past communication success rate between two nodes.

$$HIR = \frac{S_{success}}{S_{total}}$$

Where $S_{success}$ represents successful interactions and S_{total} represents total communication attempts.

The aggregated trust value T_{ij} is compared against a predefined threshold T_{th}. If the following condition holds:

$$T_{ij} > T_{th}$$

the node is considered trustworthy; otherwise, it is classified as suspicious.

3.3. Intelligent anomaly detection module

The anomaly detection system collects network data from multiple nodes and extracts behavioral features related to communication activities. These features are then processed using a classification model to determine whether a node behaves normally or maliciously. The input features used for anomaly detection include the following:

3.3.1. Traffic behavior

Traffic behavior represents patterns of packet generation and forwarding activities. Features such as packet transmission rate, packet arrival intervals, and traffic bursts are analyzed to detect abnormal patterns.

3.3.2. Routing updates

Routing updates include control packets exchanged between nodes during route discovery and maintenance. Abnormal routing updates may indicate malicious attempts to manipulate routing paths.

3.3.3. Packet transmission patterns

Packet transmission patterns capture statistics such as packet forwarding success rate, packet delay variations, and packet drop frequencies. The classification output can be expressed as:

$$C(n_i) = \begin{cases} Normal, if\ behavior\ is\ legitimate \\ Malicious, if\ anomaly\ is\ detected \end{cases}$$

Nodes identified as malicious are immediately excluded from routing operations.

3.4. Secure routing algorithm

The secure routing algorithm integrates trust evaluation and anomaly detection results to determine optimal communication paths within the network. Algorithm 1 selects nodes with high trust values and normal behavior to ensure secure packet transmission.

Algorithm 1. Multi-metric trust-based secure routing
Input: network nodes N, Trust threshold T_{th}
Output: secure routing path
1. Initialize trust values for all nodes
2. For each node n_i in network
3. Monitor packet forwarding behavior
4. Compute trust metrics (PFR, RE, PLR, CD, HIR)
5. Calculate trust score Tij
6. If $T_{ij} > T_{th}$
7. Mark node as suspicious
8. End If
9. End For
10. Collect behavioral features from nodes
11. Apply anomaly detection model
12. If node classified as malicious
13. Remove node from routing table
14. End If
15. Evaluate available routes
16. Select route with highest cumulative trust value
17. Forward packets through selected route
18. Update trust scores after each transmission

4. EXPERIMENTAL SETUP

To evaluate the effectiveness of the proposed MMTSR framework, extensive simulations were conducted to analyze its performance under varying network conditions and malicious attack scenarios in the IoT environment. The evaluation focuses on network reliability, routing efficiency, and attack detection capability. The performance of the proposed framework is compared with the classical ad hoc on-demand distance vector and a generic TBR protocol commonly used in IoT security studies. The simulation parameters used in this study are summarized in Table 1. The simulation environment considers different network sizes and malicious node ratios to examine how routing performance changes under varying security conditions.

Table 1. Simulation parameters

Parameter	Value	Description
Simulation area	1000 m×1000 m	Network deployment region
Number of nodes	50–300	IoT nodes participating in routing
Transmission range	150 m	Communication radius
Traffic type	Constant bit rate (CBR)	Packet generation pattern
Packet size	512 bytes	Data packet size
Simulation time	1000 seconds	Total simulation duration
Node mobility	Static/low mobility	IoT deployment scenario
Initial node energy	2 J	Energy capacity per node
Malicious node ratio	0–30%	Percentage of attack nodes
Routing protocols compared	AODV, TBR, and MMTSR	Performance comparison

4.1. Performance metrics

Several standard network performance metrics were used to evaluate the effectiveness of the proposed routing framework. These metrics measure both communication efficiency and attack detection performance. Packet delivery ratio measures the proportion of successfully delivered packets to the total packets sent. The variation of PDR with increasing malicious nodes is presented in Table 2.

$$PDR = \frac{Packets\ Received}{Packets\ Sent} \times 100$$

Table 2. Packet delivery ratio comparison

Malicious nodes (%)	AODV (%)	TBR (%)	Proposed MMTSR (%)
0	98.5	98.8	99.2
5	93.1	95.4	97.8
10	88.6	92.1	96.3
15	82.9	88.7	94.5
20	77.5	85.2	92.7
25	71.4	80.6	90.3
30	66.9	76.2	87.9

The results show that the proposed MMTSR framework maintains a significantly higher packet delivery ratio compared with existing protocols, particularly when the number of malicious nodes increases. Throughput represents the total amount of successfully delivered data within the network over time as as shown in Figure 1.

$$Throughput = \frac{Total\ Data\ Received}{Simulation\ Time}$$

The throughput performance of different routing protocols is presented in Table 3.

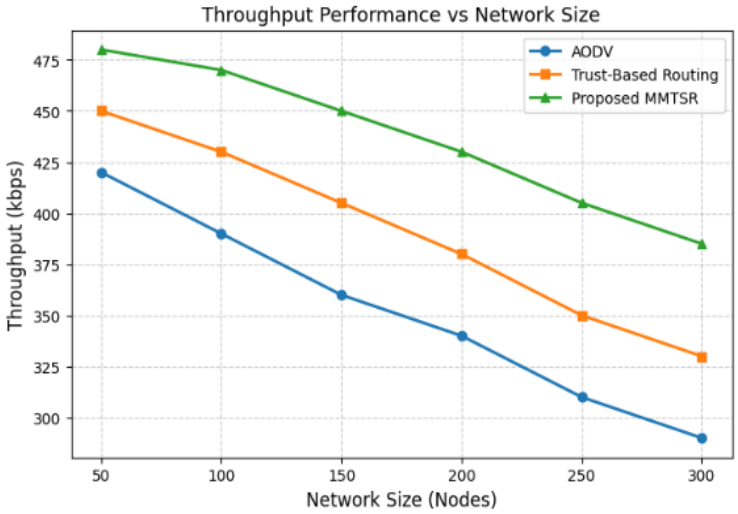


Figure 1. Throughput performance

Table 3. Network throughput comparison

Network size (Nodes)	AODV (kbps)	TBR (kbps)	Proposed MMTSR (kbps)
50	420	450	480
100	390	430	470
150	360	405	450
200	340	380	430
250	310	350	405
300	290	330	385

End-to-end delay measures the average time required for packets to travel from source to destination as shown in Figure 2.

$$Delay = \frac{\sum(t_{receive} - t_{send})}{total\ packets}$$

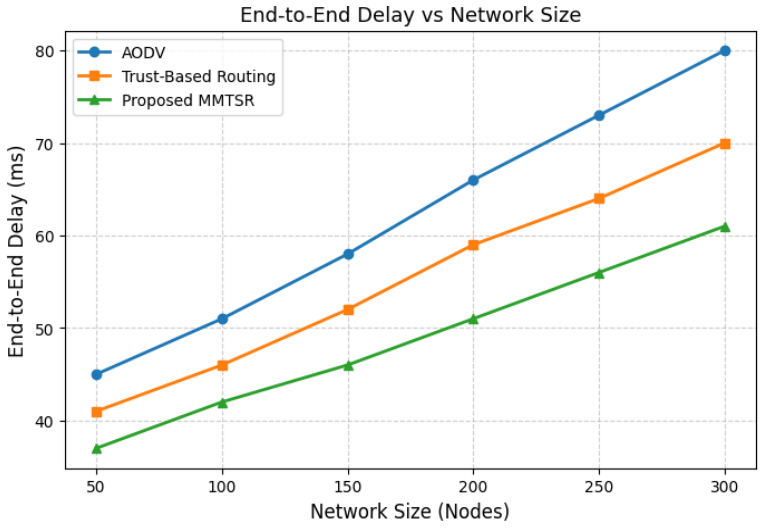


Figure 2. Delay analysis

Table 4 presents the end-to-end delay performance of AODV, TBR, and the proposed MMTSR framework under varying network sizes. As the number of nodes increases from 50 to 300, the end-to-end delay rises for all routing protocols due to increased network congestion, routing overhead, and packet forwarding complexity. However, the proposed MMTSR consistently achieves the lowest delay across all network sizes. For a network size of 50 nodes, MMTSR records a delay of 37 ms, compared to 41 ms for TBR and 45 ms for AODV. As the network expands to 300 nodes, the delay increases to 61 ms for MMTSR, while TBR and AODV experience higher delays of 70 ms and 80 ms, respectively. This demonstrates that MMTSR maintains more efficient routing performance even under dense network conditions. The superior performance of MMTSR can be attributed to its multi-metric trust evaluation mechanism, which proactively identifies reliable forwarding nodes and avoids unstable or malicious routes. Additionally, the anomaly detection module reduces routing disruptions by detecting suspicious network behavior before route establishment, thereby minimizing packet retransmissions and route recovery operations. The delay improvement becomes more significant as network size increases, indicating that MMTSR scales effectively and provides enhanced routing efficiency in large-scale IoT environments. The routing overhead comparison is presented in Table 5.

Table 4. End-to-end delay analysis

Network size	AODV (ms)	TBR (ms)	Proposed MMTSR (ms)
50	45	41	37
100	51	46	42
150	58	52	46
200	66	59	51
250	73	64	56
300	80	70	61

Table 5. Routing overhead comparison

Network size	AODV	TBR	Proposed MMTSR
50	115	108	102
100	146	138	125
150	180	165	150
200	215	195	176
250	246	220	198
300	278	250	224

Table 5 compares the routing overhead generated by AODV, TBR, and the proposed MMTSR framework for different network sizes. As the network size increases from 50 to 300 nodes, routing overhead rises for all protocols due to the increased number of route discovery processes, control packet exchanges, and network management operations. However, MMTSR consistently produces the lowest routing overhead across all network configurations. At 50 nodes, MMTSR generates a routing overhead of 102 packets, compared to 108 packets for TBR and 115 packets for AODV. As the network size increases to 300 nodes, the overhead rises to 224 packets for MMTSR, while TBR and AODV incur significantly higher overheads of 250 and 278 packets, respectively. This indicates that the proposed framework manages routing information more efficiently, even in large-scale IoT environments.

The reduced routing overhead achieved by MMTSR is primarily due to its multi-metric trust evaluation and anomaly detection mechanisms. By selecting highly trusted nodes and filtering potentially malicious or unreliable nodes during route formation, the framework minimizes route failures and reduces the need for frequent route rediscovery processes. Furthermore, the anomaly detection module prevents unnecessary control packet generation caused by malicious routing activities, thereby lowering communication overhead. As network density increases, the advantage of MMTSR becomes more pronounced, demonstrating its scalability and effectiveness in maintaining efficient routing operations.

Lower routing overhead in the proposed method indicates improved routing efficiency. Energy efficiency is critical in IoT networks due to the limited battery capacity of sensor devices. The total energy consumed by the network during the simulation is shown in Table 6. The proposed system consumes less energy due to optimized routing decisions. The anomaly detection performance of the proposed framework is presented in Table 7.

Table 6. Energy consumption analysis

Network size	AODV (J)	TBR (J)	Proposed MMTSR (J)
50	0.72	0.65	0.58
100	0.98	0.89	0.77
150	1.23	1.10	0.95
200	1.48	1.32	1.14
250	1.71	1.55	1.33
300	1.95	1.78	1.51

Table 7. Anomaly detection performance

Attack type	Detection accuracy (%)	False positive rate (%)	Detection time (ms)
Blackhole attack	97.8	2.1	24
Selective forwarding	96.4	2.8	27
Sybil attack	95.9	3.2	29
Packet dropping	96.7	2.5	26

Among the evaluated attacks, the blackhole attack achieves the highest detection accuracy of 97.8%, with a low false positive rate of 2.1% and a detection time of 24 ms. This indicates that the anomaly detection mechanism can effectively identify nodes that intentionally drop packets after attracting network traffic. For selective-forwarding attacks, the framework achieves a detection accuracy of 96.4% with a false positive rate of 2.8%, demonstrating its capability to detect nodes that selectively discard packets to disrupt communication. The proposed model also performs effectively against Sybil attacks, achieving a detection accuracy of 95.9% and a false positive rate of 3.2%.

5. CONCLUSION

This study proposed an MMTSR framework to enhance secure, reliable, and energy-efficient communication in IoT networks. The framework integrates a multi-metric trust evaluation model with a machine learning-based anomaly detection module, enabling proactive identification and isolation of malicious nodes while selecting high-trust nodes for routing. The trust evaluation considers five weighted metrics—PFR, RE, PLR, CD, and HIR—producing a comprehensive trust score that guides secure path selection. Quantitative simulation results demonstrate that the proposed framework significantly outperforms conventional protocols. Under a scenario with 10% malicious nodes, MMTSR achieves a packet delivery ratio of 97.8%, compared to 88.6% for AODV and 92.1% for traditional TBR. The average network throughput reaches 470 kbps, compared to 360 kbps and 405 kbps, respectively. The average end-to-end delay is reduced to 46 ms, while AODV and TBR exhibit delays of 58 ms and 52 ms. Routing overhead is lower at 150 control packets for 150 nodes, compared to 180 and 165, while energy consumption per node is minimized to 0.95 J, compared to 1.23 J and

1.10 J. Comparative evaluation further confirms that MMTSR provides superior detection accuracy, packet delivery performance, and overall network reliability when compared with existing secure routing approaches. These findings demonstrate the effectiveness of integrating trust evaluation and machine learning for robust IoT security. Future research will focus on extending the framework to address diverse network attack scenarios, adaptive trust management mechanisms, and large-scale heterogeneous IoT environments.

FUNDING INFORMATION

Authors state no funding involved.

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
Sangeetha Krishnaswamy	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Arulanandam Karalagan	✓		✓	✓			✓			✓	✓		✓	✓

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

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] A. B. F. Khan, "An Enhanced Multi Attribute Based Trusted Attack Resistance (EMBTR) for the Secure Routing of Sensor Nodes in Wireless Sensor Network," *Wireless Personal Communications*, vol. 137, no. 4, pp. 2397–2407, 2024, doi: 10.1007/s11277-024-11504-6.

[2] G. Altangerel, M. Tejfel, and E. Tsogbaatar, "A 1D CNN-based model for IoT anomaly detection using INT data," in *2022 IEEE 16th International Scientific Conference on Informatics (Informatics)*, Poprad, Slovakia, 2022, pp. 106-113, doi: 10.1109/Informatics57926.2022.10083469.

[3] A. B. F. Khan, H. R. Lalitha, S. K. Devi, and C. N. Rajalakshmi, "A multi-attribute based trusted routing for embedded devices in MANET-IoT," *Microprocessors and Microsystems*, vol. 89, p. 104446, Mar. 2022, doi: 10.1016/j.micpro.2022.104446.

[4] S. Gali and V. Nidumolu, "An intelligent trust sensing scheme with metaheuristic based secure routing protocol for Internet of Things," *Cluster Computing*, vol. 25, pp. 1779–1789, 2022, doi: 10.1007/s10586-021-03473-3.

[5] M. S. Gowtham, M. Ramkumar, S. S. Jamaesha, and M. Vigenesh, "Artificial self-attention rabbits battle royale multiscale network based robust and secure data transmission in mobile Ad Hoc networks," *Computers and Security*, vol. 142, 2024, doi: 10.1016/j.cose.2024.103889.

[6] D. Li, D. Cheng, J. Qin, S. Liu, and P. Liu, "EHPSO: An enhanced hybrid particle swarm optimization algorithm for internet of things," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 14, no. 6, pp. 203–211, 2018, doi: 10.3991/ijoe.v14i06.8305.

[7] S. Liu, N. Xu, N. Zhao, and L. Zhang, "Observer-based optimal fault-tolerant tracking control for input-constrained interconnected nonlinear systems with mismatched disturbances," *Optimal Control Applications and Methods*, vol. 45, no. 6, pp. 2572–2595, Nov. 2024, doi: 10.1002/oca.3173.

[8] V. Nivedita, C. S. Shieh, and M. F. Horng, "An integrated trust-based secure routing with intrusion detection for mobile Ad Hoc network using adaptive snow geese optimization algorithm," *Ain Shams Engineering Journal*, vol. 16, no. 7, 2025, doi: 10.1016/j.asej.2025.103385.

[9] R. Reka, R. Karthick, R. S. Ram, and G. Singh, "Multi head self-attention gated graph convolutional network based multi-attack intrusion detection in MANET," *Computers & Security*, vol. 136, p. 103526, Jan. 2024, doi: 10.1016/j.cose.2023.103526.

[10] B. Subramaniam *et al*., "Enhanced detection of network intrusions and anomalies in Internet of Things applications using a hybrid artificial intelligence model combining CNN and LSTM," *Scientific Reports*, vol. 16, 2026, doi: 10.1038/s41598-026-53602-4.

[11] K. Rui, H. Pan, and S. Shu, "Secure routing in the internet of things (IoT) with intrusion detection capability based on software-defined networking (SDN) and machine learning techniques," *Scientific Reports*, vol. 13, no. 1, p. 18003, Oct. 2023, doi: 10.1038/s41598-023-44764-6.
[12] Z. Shoaei, R. Esmaeilyfard, R. Javidan, and A. Jalili, "A new adaptive neuro-fuzzy TBR for dynamic IoT networks," *Cluster Computing*, vol. 28, no. 11, p. 710, Oct. 2025, doi: 10.1007/s10586-025-05381-2.
[13] N. Sivanesan, A. Rajesh, S. Anitha, and K. S. Archana, "Detecting Distributed Denial of Service (DDoS) in MANET Using Ad Hoc On-Demand Distance Vector (AODV) with Extra Tree Classifier (ETC)," *Iranian Journal of Science and Technology - Transactions of Electrical Engineering*, vol. 48, no. 2, pp. 645–659, 2024, doi: 10.1007/s40998-023-00678-7.
[14] T. Fu, S. Hao, Q. Chen, Z. Yan, H. Liu, and A. Rezaeipanah, "An energy-aware secure routing scheme in internet of things networks via two-way trust evaluation," *Pervasive and Mobile Computing*, vol. 105, p. 101995, Dec. 2024, doi: 10.1016/j.pmcj.2024.101995.
[15] C. Thai, V. N. Q. Bao, and U. H. T. Thai, "Security for Multi-hop Communication of Two-tier Wireless Networks with Different Trust Degrees," *REV Journal on Electronics and Communications*, vol. 12, no. 3–4, 2023, doi: 10.21553/rev-jec.319.
[16] W. Tian *et al.*, "A Centralized Control-Based Clustering Scheme for Energy Efficiency in Underwater Acoustic Sensor Networks," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 2, pp. 668–679, 2023, doi: 10.1109/TGCN.2023.3249208.
[17] R. Venketesh and K. Sasikala, "The design of an intrusion detection system in MANET using the IGWO-ANN classification algorithm," *International Journal of Networking and Virtual Organisations*, vol. 31, no. 1, pp. 22–42, 2024, doi: 10.1504/IJNVO.2024.141554.
[18] E. Wang, Y. Yang, J. Wu, W. Liu, and X. Wang, "An efficient prediction-based user recruitment for mobile crowdsensing," *IEEE Transactions on Mobile Computing*, vol. 17, no. 1, pp. 16–28, 2018, doi: 10.1109/TMC.2017.2702613.
[19] Y. Wang *et al.*, "Wireless Multiferroic Memristor with Coupled Giant Impedance and Artificial Synapse Application," *Advanced Electronic Materials*, vol. 8, no. 10, 2022, doi: 10.1002/aelm.202200370.
[20] Y. Yang, F. Bai, Z. Yu, T. Shen, Y. Liu, and B. Gong, "An Anonymous and Supervisory Cross-chain Privacy Protection Protocol for Zero-trust IoT Application," *ACM Transactions on Sensor Networks*, vol. 20, no. 2, 2024, doi: 10.1145/3583073.
[21] S. Zhang *et al.*, "Deep Transfer Learning for City-scale Cellular Traffic Generation through Urban Knowledge Graph," *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 4842–4851, 2023, doi: 10.1145/3580305.3599801.
[22] D. Zhou, M. Sheng, C. Bao, Q. Hao, S. Ji, and J. Li, "6G Non-Terrestrial Networks-Enhanced IoT Service Coverage: Injecting New Vitality into Ecological Surveillance," *IEEE Network*, vol. 38, no. 4, pp. 63–71, 2024, doi: 10.1109/MNET.2024.3382246.
[23] A. Fatani, A. Dahou, M. A. A. Al-Qaness, S. Lu, and M. A. Elaziz, "Advanced feature extraction and selection approach using deep learning and aquila optimizer for iot intrusion detection system," *Sensors*, vol. 22, no. 1, p. 140, Dec. 2022, doi: 10.3390/s22010140.
[24] A. B. F. Khan, D. Weslin, M. D. Babu, and M. M. Hussain, "Trust-based intelligent scheme for mitigating black hole attacks in IoT," *Journal of Harbin Institute Of Technology (New Series)*, vol. 31, no. 3, pp. 39–50, 2024, doi: 10.11916/j.issn.1005-9113.2023068.
[25] G. K. Ragesh and A. Kumar, "Trust-based secure routing and message delivery protocol for signal processing attacks in IoT applications," *Journal of Supercomputing*, vol. 79, no. 3, pp. 2882–2909, 2023, doi: 10.1007/s11227-022-04766-z.
[26] L. Yu, G. Xu, Z. Wang, N. Zhang, and F. Wei, "A Hybrid Opportunistic IoT Secure Routing Strategy Based on Node Intimacy and Trust Value," *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/6343764.

BIOGRAPHIES OF AUTHORS



Sangeetha Krishnaswamy is a research scholor at Thiruvalluvar University. She is also working as assistant professor in the Department of Computer Science at Adhiparasakthi College of Arts and Science, with over 8.6 years of teaching experience. She holds a Bachelor of Computer Application (BCA) degree from Thiruvalluvar University (2010), a Master of Computer Application (MCA) from Anna University (2015), and an M.Phil. in Computer Science from Thiruvalluvar University (2017), all achieved with first-class distinctions. Additionally, she has a B.Ed. in Computer Science from Tamil Nadu Teachers Education University with distinction. She can be contacted at email: sangeetha19892005@gmail.com.



Dr. Arulanandam Karalagan is working as an associate professor and head in the Department of Computer Science, Government Thirumagal Mills College, Gudiyattam, India. He has been engaged in research and teaching for more than 24 years. He has published several papers is reputed national and international journals. He has published several books and book Chapters. He is life membership in various professional bodies. He is member in university and college academic bodies. His main area of interest includes computer networks, internet of things, data mining, and machine learning. He can be contacted at email: arulatgtmc@gmail.com.