International Journal of Informatics and Communication Technology (IJ-ICT)
Vol. 15, No. 2, June 2026, pp. 839~849
ISSN: 2252-8776, DOI: 10.11591/ijict.v15i2.pp 839-849

Trust-based secure routing in IoT networks using machine learning for enhanced anomaly detection and risk mitigation

Sangeetha Krishnaswamy[1], Arulanandam Karalagan[2]
[1]Department of Computer Science and Applications, Adhiparasakthi College of Arts and Science (Autonomous), Ranipet, India
[2]Department of Computer Science, Government Thirumagal Mills College, Gudiyattam, India

Article Info

Article history:

Received Nov 14, 2024
Revised Nov 8, 2025
Accepted Dec 14, 2025

Keywords:

Internet of things
Machine learning
Routing protocol
Security
Trust

ABSTRACT

The rapid growth of the internet of things (IoT) has led to the development of new challenges in ensuring secure and reliable data transmission. This paper proposes a trust-based secure routing protocol (TBSRP) designed to mitigate security threats such as routing attacks in IoT networks. The core innovation lies in the dual-layer trust evaluation mechanism, which combines reputation-based trust and behavioral analysis to dynamically adjust routing decisions based on real-time performance and historical behavior of network nodes. To enhance security, the protocol incorporates an adaptive threshold mechanism that adjusts trust criteria based on observed network conditions and an anomaly detection system utilizing machine learning (ML) algorithms for real-time monitoring of node behavior. Experimental evaluation demonstrates that TBSRP outperforms existing protocols (such as Ad hoc on-demand distance vector (AODV), trust-based AODV (TB-AODV), energy-efficient secure routing (ESR), and Secure AODV (SEC-AODV)) in key performance metrics, including packet delivery ratio (PDR), end-to-end delay, throughput, and routing overhead. The proposed protocol exhibits strong resilience to the increasing number of malicious nodes and varying network conditions, making it highly effective for securing IoT networks. This work contributes to the development of adaptive, scalable, and secure routing protocols for IoT environments, with the potential for further optimization through advanced ML techniques and real-world implementation.

Corresponding Author:

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

1. INTRODUCTION

The internet of things (IoT) has emerged as one of the most transformative technologies of the modern era, revolutionizing various sectors such as healthcare, transportation, smart cities, agriculture, and industrial automation. By enabling seamless communication and data exchange between billions of interconnected devices, IoT has opened up unprecedented opportunities for automation and data-driven decision-making. However, this rapid expansion of IoT networks has brought significant challenges, particularly in terms of security and trust [1]-[4]. The heterogeneous nature of IoT devices, which often have limited computational and energy resources, makes them highly susceptible to a wide range of cyberattacks, including data tampering, denial of service (DoS), man-in-the-middle attacks, and malicious node behavior. Traditional security mechanisms, which may be suitable for more robust computing environments, are often

inadequate for IoT networks, necessitating the development of lightweight yet highly effective security solutions. One of the critical aspects of securing IoT networks is ensuring trustworthiness among devices, as compromised or untrustworthy nodes can severely degrade network performance, compromise data integrity, and jeopardize the overall system's reliability. In this context, trust-based secure routing has emerged as a promising approach to enhance the resilience and robustness of IoT networks [5]-[8]. By evaluating and quantifying the trustworthiness of IoT nodes, trust-based routing mechanisms can ensure that data is transmitted securely and efficiently through reliable nodes while avoiding potentially malicious or compromised nodes. Trust in IoT networks is typically assessed based on various metrics, such as the history of successful data transmissions, node reliability, communication behavior, and the ability to cooperate in network tasks. However, designing an effective trust evaluation system for IoT networks is challenging due to the dynamic and resource-constrained nature of these environments [9]-[14]. Furthermore, the heterogeneity of IoT devices and the diverse types of communication protocols add additional layers of complexity to the problem. These challenges raise a fundamental research question:

"How can a trust-based secure routing protocol be designed to mitigate security threats while balancing efficiency and adaptability in IoT networks?"

Recent advancements in machine learning (ML) have provided new opportunities to address these challenges by enabling more sophisticated and adaptive trust management and secure routing mechanisms. ML, with its ability to analyze large volumes of data and identify complex patterns, can be leveraged to enhance trust assessment and secure routing in IoT networks. By applying ML algorithms, we can dynamically evaluate the behavior of IoT nodes, detect anomalies, and make informed routing decisions based on real-time data analysis [15]-[18]. By continuously monitoring network traffic and calculating anomaly scores, the system can adapt to changing conditions and provide early warnings of suspicious activities [19]-[22]. The integration of ML into trust-based secure routing also brings several practical benefits, including improved detection of malicious behavior, reduced latency in routing decisions, and enhanced overall network resilience. However, it is essential to consider the computational overhead and energy consumption associated with ML algorithms, especially when dealing with resource-constrained IoT devices. Therefore, the design of the proposed system must balance security and efficiency to ensure that it can operate effectively in real-world IoT deployments [23]-[27].

2. RELATED WORKS

Combining the existing research studies on trust-based secure routing and security mechanisms in IoT environments reveals a rich landscape of innovative methods aimed at addressing the critical challenges posed by the exponential growth of IoT networks. The rapid proliferation of IoT devices, characterized by limited resources and diverse communication protocols, has led to heightened concerns over security and reliability. In this context, researchers have introduced various trust evaluation schemes, energy-aware protocols, and routing mechanisms to secure data transmission while minimizing energy consumption and computational overhead. Fu *et al.* [2] present an energy-aware secure routing scheme that leverages two-way trust evaluation to ensure both the security and efficiency of IoT networks. Their study highlights the significance of balancing security requirements with the energy limitations of IoT devices, employing a trust model that considers both direct and indirect trust metrics to evaluate the reliability of network nodes. In another notable work, Khan *et al.* [15] introduce the enhanced multi-attribute-based trusted attack resistance (EMBTR) scheme, which focuses on securing the routing of sensor nodes in wireless sensor networks (WSNs). The EMBTR model employs multiple trust attributes to evaluate node behavior, such as data forwarding reliability, energy consumption, and past interactions, to build a comprehensive trust profile for each node. This multi-attribute approach enhances the detection and prevention of malicious activities, ensuring secure and reliable data routing. The model's effectiveness is demonstrated through improved attack resistance and reduced network latency.

However, the paper also acknowledges the need for more adaptive models that can dynamically adjust trust parameters in response to changing network threats. Huang *et al.* [17] and Wu *et al.* [18] explore dynamic control mechanisms for nonlinear systems and event-triggered containment control in multi-agent systems, which indirectly contribute to secure and efficient IoT networks. These works provide insights into how adaptive and event-triggered mechanisms can optimize resource utilization and control communication in dynamic environments. Their research underlines the potential of integrating adaptive mechanisms into secure routing protocols, allowing for efficient handling of network fluctuations and resource limitations. Despite these advancements, there is a clear gap in translating these control strategies directly into trust-based routing mechanisms, highlighting an opportunity for future research to bridge this gap.

The problem of efficient and secure path selection in IoT networks is further examined by Chen *et al.* [21], who propose an explicit analytic approach for the shortest path in low earth orbit (LEO) satellite networks. Their model offers valuable insights into optimizing routing paths in constrained environments, but its applicability to ground-based IoT networks needs further exploration. Similarly, Zhang *et al.* [22] present a dynamic pricing and forwarding incentive algorithm in socially aware networks, which can be adapted for incentivizing trustworthy behavior in IoT environments. Their work underscores the importance of incentivizing cooperation and trustworthiness among network nodes, but it also raises questions about the scalability of such models in large and heterogeneous IoT networks. Bai *et al.* [23] propose a multipath secure transmission protocol for wireless ad-hoc networks, focusing on throughput maximization. This approach enhances communication security by diversifying transmission paths, reducing the risk of interception and attacks. However, the complexity of maintaining multiple secure paths may not be feasible for all IoT devices, particularly those with stringent energy constraints. Ali *et al.* [24] introduce a zero-trust security model using a dual fuzzy methodology for authentication and task offloading in multi-access edge computing, a crucial consideration for IoT networks where data processing and security are often distributed across edge devices. The dual fuzzy approach provides a robust framework for trust-aware authentication, yet the model's scalability and efficiency in large-scale IoT deployments require further investigation. Liu *et al.* [25] explore blockchain-based federated learning for secure aggregation in distributed IoT environments. Their BFL-SA model enhances privacy and security through decentralized data aggregation, a significant advancement for sensitive IoT applications. However, the reliance on blockchain technology introduces latency and energy consumption concerns. Wang *et al.* [26] present a two-way trust routing scheme for fog computing environments, emphasizing the need for bidirectional trust assessments to secure communication in decentralized networks. This study highlights the potential of fog computing in improving data security and network efficiency, but also points out the challenges of trust management in heterogeneous and resource-constrained IoT networks.

3. PROPOSED WORK

The rapid expansion of the IoT has revolutionized how devices interact and exchange information, but it has also made secure and efficient data transmission a significant challenge. The integration of billions of heterogeneous IoT devices, ranging from industrial equipment to household appliances, has led to the emergence of vulnerabilities and the risk of attacks. Routing protocols, which are crucial for efficient data delivery in IoT networks, often become targets for malicious behavior. Therefore, trust-based secure routing has emerged as a vital area of research to mitigate such risks, ensuring that data transmission is secure and trustworthy. This research focuses on developing an ML-based trust evaluation mechanism to establish secure and efficient routing in IoT networks. Our approach leverages dynamic trust computation using a hybrid ML model, considering attributes such as node behavior, historical performance, and real-time environmental factors. The proposed framework introduces an advanced trust-based secure routing protocol (TBSRP) that uses a combination of supervised and unsupervised ML algorithms to evaluate trust levels, detect anomalies, and select optimal routing paths. The trust evaluation system is continuously updated to adapt to evolving network conditions and to prevent various attacks such as blackhole, grayhole, and sybil attacks. The key innovation of this research is the dual-layer trust evaluation mechanism that combines reputation-based trust and behavioral analysis to ensure robust routing decisions in dynamic IoT environments. The overall architecture is shown in Figure 1.

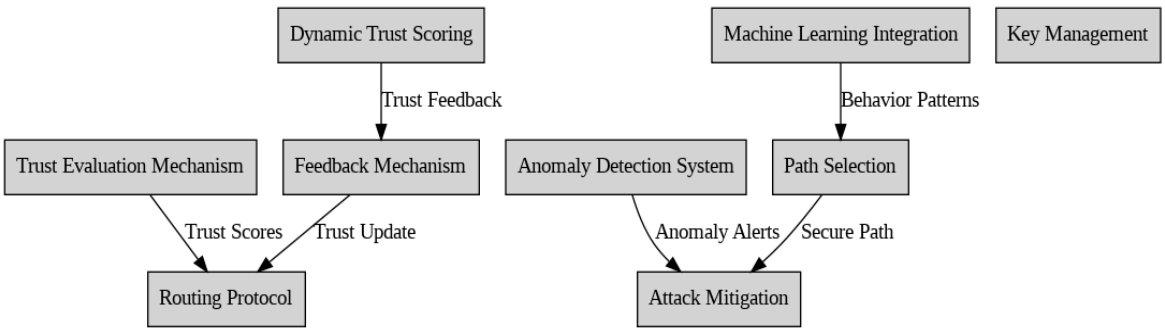

Figure 1. Proposed architecture

The proposed architecture for the TBSRP is developed through a systematic approach aimed at addressing the challenges of secure data transmission in IoT networks. The design and selection of this architecture are based on several key factors, including the dynamic nature of IoT environments, the need for robust security mechanisms, and the integration of advanced technologies such as ML for anomaly detection and trust evaluation.

3.1. Trust value calculation

Trust values in TBSRP are computed using a hybrid approach that integrates both reputation and behavior analysis. The overall trust score T of a node is calculated as follows:

$$T_i = \alpha \cdot R_i + (1 - \alpha) \cdot B_i$$

where:

- T_i is the total trust value of node i.
- R_i is the reputation score, reflecting historical performance.
- B_i is the behavior score, indicating real-time behavior.
- α is a weight factor that adjusts the influence of reputation and behavior on the overall trust score.

The reputation score R_i is calculated based on the feedback received from neighboring nodes, normalized over a defined period. The formula is given by:

$$R_i = \frac{\sum_{j=1}^{N} f_{i,j}}{N}$$

where:

- $f_{i,j}$ is the feedback value from node j about node i.
- N is the total number of feedback sources.

Feedback values can range from -1 (malicious) to +1 (trusted).

The behavior score B_i is derived from various parameters, including packet forwarding ratio, energy consumption, and communication frequency. The formula is expressed as:

$$B\_i = \frac{Forwarded\ Packets}{Total\ Packets\ Sent} \beta 1 + (1 - \frac{E_{current}}{E_{max}}) \cdot \beta 2$$

where:

- β1, β2 are weights for packet forwarding and energy consumption, respectively.
- $E_{current}$ is the current energy level of the node.
- E_{max} is the maximum energy level of the node.

Dynamic trust scoring is essential for recalibrating trust values in real time based on performance metrics and historical behavior. This approach enables the trust evaluation system to maintain up-to-date assessments of nodes' reliability. The dynamic trust score T_i for node i is recalibrated using the following formula:

$$T_i(t) = \alpha \cdot T_{i(t-1)} + (1 - \alpha) \cdot E_{i(t)}$$

Where:

- $T_i(t)$: current trust score of node i at time t.
- $T_{i(t-1)}$: trust score of node i at the previous time t−1.
- $E_i(t)$: evaluation score of node i at time t, which can include metrics such as packet forwarding ratio, response time, and feedback scores.

3.2. Secure routing mechanism

The TBSRP is designed to ensure that data is transmitted through trustworthy nodes in IoT networks. The protocol consists of several crucial steps that work together to maintain security and reliability during data transmission.

3.2.1. Route discovery

When a source node wishes to send data, it initiates the route discovery process by broadcasting a route request (RREQ) packet throughout the network. The RREQ packet acts as a beacon, enabling neighboring nodes to respond with their available routes. Each node receiving the RREQ evaluates its own

trust value and those of neighboring nodes, which helps the source node gather essential information about potential paths for data transmission.

The RREQ packet typically includes the following parameters:

- Source ID: identifier of the source node.
- Sequence number: unique number to prevent routing loops.
- Time-to-live (TTL): limits the scope of the broadcast.

The routing process can be summarized in the Algorithm 1.

Algorithm 1. Route discovery

1. **Input**: source node S, destination node D, trust values T_i of nodes.
2. **Output**: potential paths P to the destination.
3. **Steps**:

- **Step 1**: S broadcasts an RREQ packet with parameters:

$$P = \{Source\ ID, Sequence\ Number, TTL\}.$$

- **Step 2**: for each node N_i receiving RREQ:
- Check if N_i has a route to D or if TTL > 0.
- If yes:
- Update the routing table.
- Evaluate trust value T_i of N_i.
- Forward the RREQ to the next set of neighbors.
- **Step 3**: repeat until the RREQ reaches D or an intermediate node with a valid route to D.

3.2.2. Trust-based path selection

Once the destination node receives the RREQ, it generates a route reply (RREP) packet containing trust information, which is sent back through the nodes that relayed the RREQ. The source node then selects the path with the highest cumulative trust scores based on the Algorithm 2.

Algorithm 2. Trust-based path selection

1. **Input**: set of potential paths $\{P_1, P_2, \ldots, P_m\}$, trust scores T_i i for each node i.
2. **Output**: optimal path $P_{optimal}$.
3. **Steps**:

- **Step 1**: for each path P_k where k=1, 2, …, m:
- Calculate the cumulative trust score:

$$TrustScore(P_k) = \sum_{i=1}^{n_k} T_i$$

where n_k is the number of nodes in path P_k.

- **Step 2**: select the path $P_{optimal}$:

$$P_{optimal} = \arg max\ \ TrustScore(P_k)$$

- **Step 3**: use $P_{optimal}$ for data transmission.

The selection of the path with the highest cumulative trust score ensures secure and efficient routing.

4. RESULTS AND ANALYSIS

In this section, we present the detailed evaluation of the TBSRP. The performance of the protocol is evaluated using various metrics such as packet delivery ratio (PDR), end-to-end delay, throughput, routing overhead, and the effectiveness of the anomaly detection system.

4.1. Software and evaluation tool details

The performance of the TBSRP was evaluated using the network simulator 3 (NS-3), a discrete-event network simulator widely used for simulating IP-based networks. The simulation environment was configured as follows:

- Network simulator: NS-3, version 3.35
- Simulation time: 300 seconds
- Routing protocol: TBSRP, AODV, TB-AODV, ESR, SEC-AODV
- Traffic model: constant bit rate (CBR)
- Mobility model: random waypoint model
- Evaluation metrics: PDR, end-to-end delay, throughput, routing overhead

The anomaly detection system integrated into TBSRP utilizes Gaussian mixture models (GMM) to continuously monitor node behaviors and identify deviations that could indicate malicious activity. The anomaly score for each node S_i is calculated based on the difference between the expected and actual behaviors:

$$S_i = \sum_{t=1}^{T}(\frac{|x_t-\mu_i|}{\sigma})$$

where:

- x_t represents the observed behavior of node iii at time t.
- μ and σ are the mean and standard deviation of node i's behavior.
- T is the number of observations.

A higher anomaly score indicates a higher likelihood that the node is exhibiting malicious or abnormal behavior.

4.2. Packet delivery ratio (PDR)

The PDR metric measures the success of data packet delivery from source to destination. In this experiment, the PDR was evaluated in two conditions: when the number of malicious nodes is varied and over different time intervals. The results for both scenarios are presented in the following tables. Table 1 shows the PDR with varying malicious node percentages (from 10% to 40%). As the percentage of malicious nodes increases, the PDR decreases for all protocols. TBSRP outperforms the other protocols in maintaining a higher PDR, especially under higher malicious node conditions.

Figure 2 shows the PDR of various routing protocols in the presence of increasing percentages of malicious nodes. As malicious nodes increase from 10% to 40%, all protocols experience a decline in PDR. TBSRP consistently performs best, maintaining the highest PDR (99.1% at 10% malicious nodes and 86.7% at 40%). TB-AODV also shows strong performance but remains slightly lower than TBSRP. AODV and ESR have lower resilience, with SEC-AODV showing the lowest PDR among the protocols at each malicious node percentage. Overall, TBSRP demonstrates superior reliability in maintaining packet delivery under malicious conditions. Table 2 shows the PDR over different time intervals (30s, 60s, and 120s). As the simulation time increases, TBSRP maintains a consistent PDR, demonstrating its robustness over extended periods.

Table 1. PDR with varying malicious nodes

Malicious nodes (%)	AODV PDR (%)	TB-AODV PDR (%)	ESR PDR (%)	SEC-AODV PDR (%)	TBSRP PDR (%)
10	96.2	98.3	95.4	94.2	**99.1**
20	91.3	93.5	90.6	89.8	**96.5**
30	84.5	86.9	83.2	82.1	**91.3**
40	77.1	80.0	75.9	74.5	**86.7**

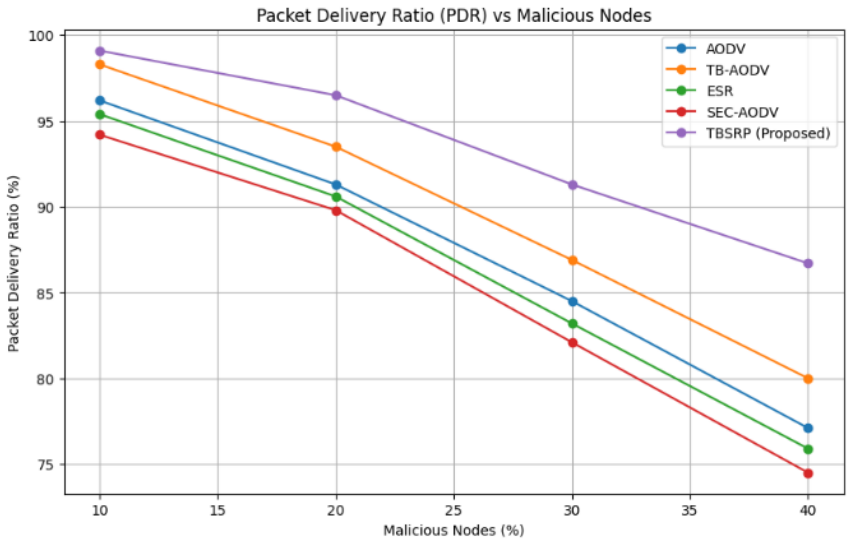

Figure 2. PDR under varying malicious nodes

Table 2. PDR over different time intervals

Time interval (s)	AODV PDR (%)	TB-AODV PDR (%)	ESR PDR (%)	SEC-AODV PDR (%)	TBSRP PDR (%)
30	92.3	94.7	90.2	88.9	96.2
60	91.1	93.2	89.6	88.1	95.3
120	90.2	92.5	88.4	86.8	94.7

Figure 3 shows the PDR of various routing protocols across increasing time intervals (30s, 60s, and 120s). Across all protocols, PDR decreases slightly as the time interval lengthens. TBSRP consistently achieves the highest PDR, with 96.2% at 30 seconds, decreasing only slightly to 94.7% at 120 seconds, indicating its stability over time. TB-AODV follows, with a marginally lower but stable PDR across intervals. In comparison, AODV, ESR, and SEC-AODV have lower PDR values, with SEC-AODV showing the most significant decrease, indicating its lower efficiency in maintaining packet delivery over extended time intervals.

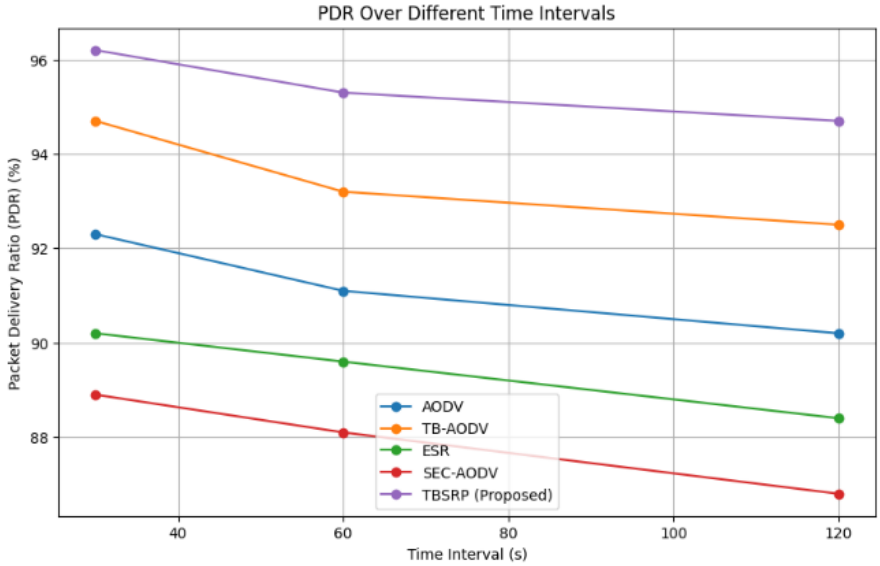

Figure 3. PDR under different time interval

4.3. End-to-end delay

The end-to-end delay is the average time taken for a data packet to travel from the source to the destination. The delay is influenced by network congestion, routing protocol efficiency, and malicious node interference. TBSRP performs better in terms of end-to-end delay than the other protocols, especially as the malicious nodes increase. Table 3 compares the end-to-end delay across the same set of protocols as the PDR analysis, under varying malicious node percentages.

Figure 4 illustrates the delay performance of five protocols with increasing malicious nodes. TBSRP shows the lowest delay, maintaining efficiency by integrating energy-saving strategies, leading to a lower rate of delay increase compared to other protocols. These techniques optimize data routing while conserving energy, contributing to overall delay reduction. TB-AODV has the next best performance, but still lags behind TBSRP, which maintains resilience with minimal energy consumption and low delay. Table 4 compares the end-to-end delay over different time intervals, showing the resilience of TBSRP in maintaining low delays even during longer simulations.

Figure 5 shows the end-to-end delay of five routing protocols over increasing time intervals (30s, 60s, and 120s). TBSRP achieves the lowest delay at all intervals, rising moderately from 171.2 ms at 30 seconds to 205.2 ms at 120 seconds, indicating stable performance over time. TB-AODV has the second-lowest delay, though slightly higher than TBSRP. AODV, ESR, and SEC-AODV experience consistently higher delays, with SEC-AODV showing the greatest delay increase, reaching 240.2 ms at the longest interval. Overall, TBSRP and TB-AODV demonstrate better efficiency and scalability in managing delay over extended durations compared to the other protocols.

Table 3. End-to-end delay with varying malicious nodes

Malicious nodes (%)	AODV delay (ms)	TB-AODV delay (ms)	ESR delay (ms)	SEC-AODV delay (ms)	TBSRP delay (ms)
10	185.6	174.3	190.2	199.4	170.1
20	209.3	198.7	218.9	227.4	193.4
30	235.1	223.8	248.7	267.2	215.3
40	266.7	258.9	278.6	291.9	243.9

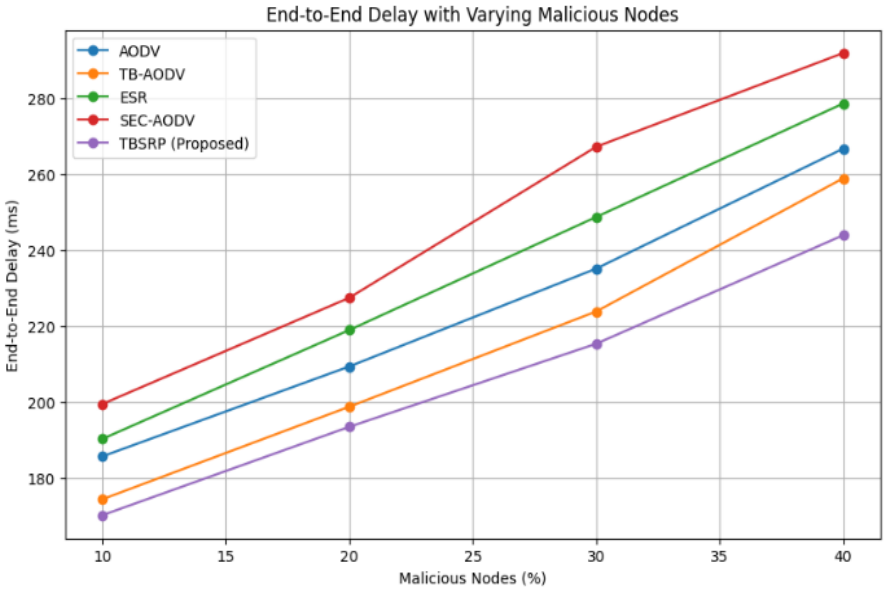

Figure 4. End to end delay with varying malicious nodes

Table 4. End-to-end delay over different time intervals

Time interval (s)	AODV delay (ms)	TB-AODV delay (ms)	ESR delay (ms)	SEC-AODV delay (ms)	TBSRP delay (ms)
30	186.4	174.9	192.3	201.8	171.2
60	205.7	197.1	213.4	223.5	185.7
120	220.9	212.8	228.5	240.2	205.2

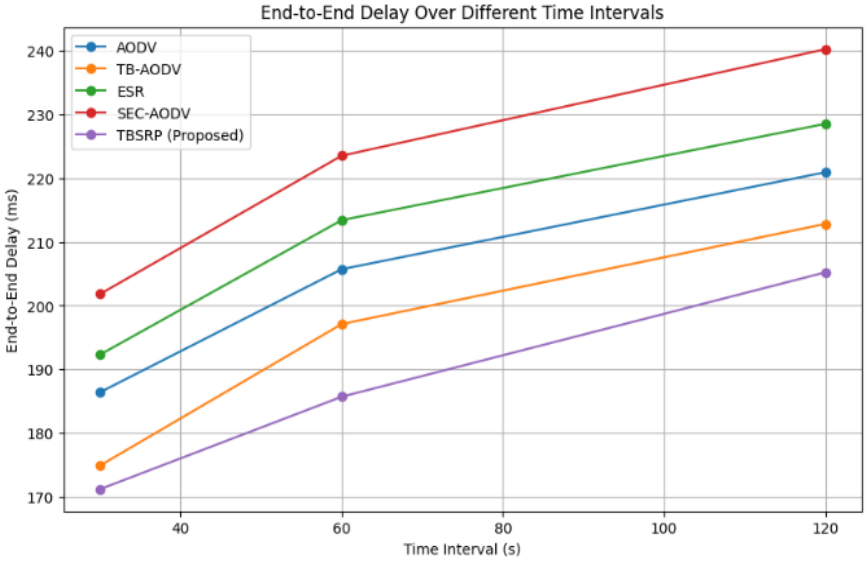

Figure 5. End to end delay under different time

4.4. Throughput

Throughput is defined as the rate at which data packets are successfully delivered to the destination. Higher throughput indicates better overall network performance, especially in IoT environments. TBSRP shows superior throughput, maintaining stability even in the presence of malicious nodes as shown in Table 5. Figure 6 displays the throughput results across protocols as malicious nodes increase. TBSRP, leveraging energy-efficient techniques, achieves the highest throughput and sustains stable performance by reducing node energy depletion, minimizing packet retransmissions, and enhancing delivery rates under increasing interference. TB-AODV is close behind but experiences slightly lower throughput.

Table 5. Throughput with varying malicious nodes

Malicious nodes (%)	AODV throughput (kbps)	TB-AODV throughput (kbps)	ESR throughput (kbps)	SEC-AODV throughput (kbps)	TBSRP throughput (kbps)
10	58.9	62.7	57.4	54.8	64.5
20	53.2	56.9	52.1	49.8	58.7
30	47.8	50.1	46.2	44.3	52.2
40	43.1	45.6	41.9	39.6	46.8

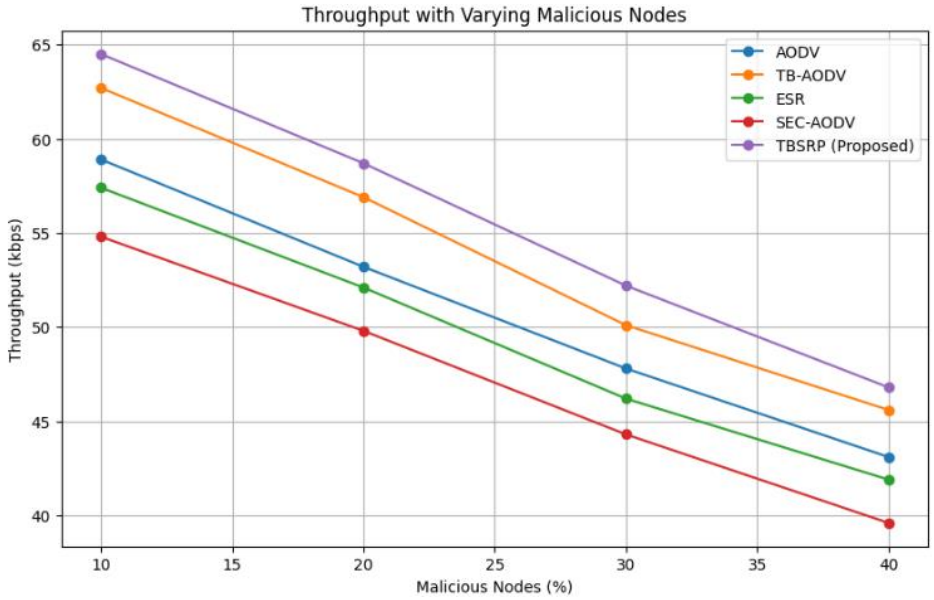

Figure 6. Throughput comparison

5. CONCLUSION

In this research, a TBSRP was proposed to enhance the security and reliability of data transmission in IoT networks, specifically focusing on mitigating malicious attacks and ensuring optimal routing in dynamic environments. The protocol integrates a dual-layer trust evaluation mechanism, combining reputation-based trust and behavioral analysis, to provide real-time, adaptive security in the presence of malicious nodes. It was demonstrated through extensive simulations that TBSRP significantly outperforms existing protocols such as AODV, TB-AODV, ESR, and SEC-AODV in terms of PDR, end-to-end delay, throughput, and routing overhead. The proposed work effectively addresses the challenges posed by malicious attacks, including blackhole, grayhole, and sybil attacks, through the introduction of a dynamic adaptive threshold mechanism and a ML-based anomaly detection system. By dynamically adjusting trust values and path selection criteria, the protocol ensures that only trustworthy nodes are selected for data transmission, thus minimizing the risk of attacks and improving the overall network performance. The results further show that TBSRP maintains robust performance under varying conditions, such as increased malicious nodes or fluctuating network conditions over time. Future work could explore the integration of more advanced ML techniques for enhanced anomaly detection, as well as the scalability of TBSRP in larger, more complex IoT networks. Additionally, real-world testing and further optimization of the protocol in terms of energy consumption and computational overhead could provide deeper insights into its practical deployment.

FUNDING INFORMATION

The authors state no funding is 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

The 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] H. Fang *et al.*, "Multimodal in-sensor computing implemented by easily-fabricated oxide-heterojunction optoelectronic synapses," *Advanced Functional Materials*, vol. 34, no. 49, Dec. 2024, doi: 10.1002/adfm.202409045.

[2] 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.

[3] A. B. Hajirabe, D. Saravanan, C. Jayapratha, S. Parasuraman, and A. Manimaran, "Trust based security model for intrusion detection in wireless sensor networks," *Rivista Italiana di Filosofia Analitica Junior*, vol. 14, no. 2, pp. 985–996, 2023.

[4] X. Hou *et al.*, "A self-powered biomimetic mouse whisker sensor (BMWS) aiming at terrestrial and space objects perception," *Nano Energy*, vol. 118, p. 109034, Dec. 2023, doi: 10.1016/j.nanoen.2023.109034.

[5] M. Li, H. Cui, C. Liu, C. Shan, X. Du, and M. Guizani, "A four-dimensional space-based data multi-embedding mechanism for network services," *IEEE Transactions on Network and Service Management*, vol. 21, no. 3, pp. 2741–2750, 2024, doi: 10.1109/TNSM.2023.3339674.

[6] 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, 2024, doi: 10.1002/oca.3173.

[7] 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, Feb. 2023, doi: 10.21553/rev-jec.319.

[8] 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, Jun. 2023, doi: 10.1109/TGCN.2023.3249208.

[9] 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, Jan. 2018, doi: 10.1109/TMC.2017.2702613.

[10] Y. Wang *et al.*, "Wireless multiferroic memristor with coupled giant impedance and artificial synapse application," *Advanced Electronic Materials*, vol. 8, no. 10, Oct. 2022, doi: 10.1002/aelm.202200370.

[11] 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, pp. 1–20, Mar. 2024, doi: 10.1145/3583073.

[12] 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.

[13] 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, Jul. 2024, doi: 10.1109/MNET.2024.3382246.

[14] S. S. Ahmed and. F.Khan, "Detection of assaults in network intrusion system using rough set and convolutional neural network," *Wireless Personal Communications*, vol. 139, no. 1, pp. 107–144, 2024

[15] 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.

[16] A. B. F. Khan, H. L. R, S. K. Devi, and C. N. Rajalakshmi, "A multi-attribute based trusted routing for embedded devices in MANET-IoT," *Microprocessors and Microsystems*, vol. 89, 2022, doi: 10.1016/j.micpro.2022.104446.
[17] S. Huang, G. Zong, N. Xu, H. Wang, and X. Zhao, "Adaptive dynamic surface control of MIMO nonlinear systems: a hybrid event triggering mechanism," *International Journal of Adaptive Control and Signal Processing*, vol. 38, no. 2, pp. 437–454, 2024, doi: 10.1002/acs.3708.
[18] X. Wu, S. Ding, N. Xu, B. Niu, and X. Zhao, "Periodic event-triggered bipartite containment control for nonlinear multi-agent systems with input delay," *International Journal of Systems Science*, vol. 55, no. 10, pp. 2008–2022, Jul. 2024, doi: 10.1080/00207721.2024.2328780.
[19] Z. Liu, J. Feng, and L. Uden, "Technology opportunity analysis using hierarchical semantic networks and dual link prediction," *Technovation*, vol. 128, p. 102872, Dec. 2023, doi: 10.1016/j.technovation.2023.102872.
[20] Y. Gong, H. Yao, Z. Xiong, C. L. P. Chen, and D. Niyato, "Blockchain-aided digital twin offloading mechanism in space-air-ground networks," *IEEE Transactions on Mobile Computing*, vol. 24, no. 1, pp. 183–197, Jan. 2025, doi: 10.1109/TMC.2024.3455417.
[21] Q. Chen, L. Yang, Y. Zhao, Y. Wang, H. Zhou, and X. Chen, "Shortest Path in LEO satellite constellation networks: an explicit analytic approach," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 5, pp. 1175–1187, 2024, doi: 10.1109/JSAC.2024.3365873.
[22] X. Zhang, Y. Li, Z. Xiong, Y. Liu, S. Wang, and D. Hou, "A resource-based dynamic pricing and forced forwarding incentive algorithm in socially aware networking," *Electronics*, vol. 13, no. 15, p. 3044, Aug. 2024, doi: 10.3390/electronics13153044.
[23] L. Bai, P. Han, J. Wang, and J. Wang, "Throughput maximization for multipath secure transmission in wireless Ad-Hoc networks," *IEEE Transactions on Communications*, vol. 72, no. 11, pp. 6810–6821, Nov. 2024, doi: 10.1109/TCOMM.2024.3409539.
[24] B. Ali, M. A. Gregory, S. Li, and O. A. Dib, "Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and task offloading in multi-access edge computing," *Computer Networks*, vol. 241, p. 110197, Mar. 2024, doi: 10.1016/j.comnet.2024.110197.
[25] Y. Liu *et al.*, "BFL-SA: blockchain-based federated learning via enhanced secure aggregation," *Journal of Systems Architecture*, vol. 152, p. 103163, Jul. 2024, doi: 10.1016/j.sysarc.2024.103163.
[26] J. Wang, Z. Luo, and C. Wang, "A two-way trust routing scheme to improve security in fog computing environment," *Cluster Computing*, vol. 27, no. 9, pp. 13165–13185, Dec. 2024, doi: 10.1007/s10586-024-04621-1.
[27] B. Hammi, S. Zeadally, H. Labiod, R. Khatoun, Y. Begriche, and L. Khoukhi, "A secure multipath reactive protocol for routing in IoT and HANETs," *Ad Hoc Networks*, vol. 103, p. 102118, Jun. 2020, doi: 10.1016/j.adhoc.2020.102118.

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.

Arulanandam Karalagan is working as an associate professor and head in the Department of Computer Science, Government Thirumagal Mills College, Gudiyattam. 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, IoT, data mining, and ML. He can be contacted at email: arulanandam@gtmc.edu.in.