sciendo INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS

Research Article | DOI: 10.2478/ijssis-2025-0032 Issue 1 | Vol. 18 (2025)

Adaptive trust-based secure routing protocol with reinforced anomaly detection for IoT networks

K. Sangeetha[1,*] and K. Arulanandam[2]

[1]Department of Computer Science and Applications, Adhiparasakthi College of Arts and Science (Autonomous), (Affiliated to Thiruvalluvar university, Vellore), Ranipet, Tamil Nadu, India

[2]Department of Computer Science, Government Thirumagal Mills College, (Affiliated to Thiruvalluvar university, Vellore), Gudiyattam, Tamil Nadu, India

*E-mail: sangeetha19892005@gmail.com

Received for publication Janurary 10, 2025.

Abstract

The increasing deployment of Internet of Things (IoT) networks has made them a target for sophisticated routing attacks, including blackhole, Sybil, rank, and wormhole attacks. To address these challenges, this paper proposes the adaptive trust-based secure routing protocol (ATBSRP), a novel framework that integrates trust evaluation, anomaly detection, and lightweight cryptographic mechanisms to enhance secure communication in IoT environments. The trust evaluation module dynamically assesses node behavior based on direct interactions, indirect recommendations, and historical trust scores, ensuring accurate and up-to-date trust values. The anomaly detection module uses a hybrid approach combining behavioral analysis, Gaussian mixture model (GMM)-based detection, and machine learning classifiers to effectively identify and mitigate malicious activities. Additionally, a lightweight cryptographic mechanism using elliptic curve cryptography (ECC), one-time hash chains, and a challenge-response mechanism safeguard data transmission with minimal computational overhead. The adaptive trust-based routing mechanism selects routes based on threshold-based trust scoring, ensures dynamic path adaptation in case of compromised nodes, and incorporates quality of service (QoS)-aware routing to maintain network efficiency. Experimental evaluations demonstrate that ATBSRP outperforms existing approaches in terms of packet delivery ratio (PDR), end-to-end delay, throughput, routing overhead, and detection accuracy. The proposed framework offers a scalable, secure, and efficient solution for mitigating routing threats in IoT networks, ensuring reliable data transmission while minimizing network overhead.

Keywords

ATBSRP, routing attacks, machine learning, IoT, security

I. Introduction

The rapid advancement of the Internet of Things (IoT) has led to the widespread adoption of interconnected smart devices across various domains, including smart health care, industrial automation, environmental monitoring, smart homes, and intelligent transportation systems. IoT networks facilitate seamless data exchange and automation, thereby enhancing operational efficiency and enabling real-time decision-making. However, the unique characteristics of IoT, such as decentralized architectures, resource constraints, heterogeneous devices, and reliance on wireless communication, expose them to a wide range of security vulnerabilities. Unlike traditional networks, IoT environments lack robust centralized security mechanisms, making them highly susceptible to malicious attacks that can compromise

data integrity, network availability, and user privacy [1–4]. Among the numerous security threats, routing attacks pose a significant challenge as they directly impact the data transmission process, leading to packet loss, misdirection of traffic, unauthorized access, and service disruptions. Blackhole attacks, gray hole attacks, wormhole attacks, Sybil attacks, and selective forwarding attacks are among the most prominent threats targeting IoT routing protocols. In a blackhole attack, malicious nodes absorb all network traffic by falsely advertising optimal routes, causing severe packet loss. Similarly, in a gray hole attack, attackers selectively drop packets, making detection difficult. Wormhole attacks exploit routing vulnerabilities by creating fake tunnels between distant nodes to manipulate routing decisions, while Sybil attacks involve an adversary forging multiple fake identities to influence trust-based decisions. Additionally, selective forwarding attacks occur when compromised nodes drop specific packets instead of forwarding them, resulting in data loss and network inefficiency. These attacks undermine the reliability of IoT networks and hinder their ability to support critical applications that demand secure and efficient communication [5–8].

To counter these security challenges, several trust-based secure routing protocols (TBSRP) have been proposed in recent years, aiming to detect and mitigate malicious activities in IoT networks. Existing solutions, such as Ad hoc On-Demand Distance Vector (AODV), Trust-Based AODV (TB-AODV), Energy-Efficient Secure Routing (ESR), and Secure AODV (SEC-AODV), use various mechanisms to enhance security while maintaining network performance. Traditional security approaches rely on cryptographic techniques and authentication mechanisms to protect data transmission, but these solutions often introduce significant computational overhead, making them unsuitable for resource-constrained IoT devices [9–12]. Trust-based routing protocols, on the other hand, assess node behavior over time to establish a trust score, enabling the identification of malicious nodes based on their historical actions. However, existing trust-based solutions suffer from limitations such as static trust thresholds, susceptibility to insider attacks, high false-positive rates, and lack of adaptability to dynamic network conditions. Many protocols fail to effectively detect sophisticated attacks, particularly Sybil and wormhole attacks, as adversaries can manipulate trust scores by behaving normally for an extended period before launching an attack [13–16]. Additionally, the reliance on predefined trust evaluation criteria makes existing protocols less effective in handling evolving security threats in IoT networks. Therefore, there is a need for an adaptive, intelligent, and lightweight TBSRP that can dynamically adjust its security mechanisms based on the changing behavior of network nodes.

The increasing complexity and heterogeneity of IoT networks further exacerbate security challenges, making it imperative to develop advanced intrusion detection mechanisms that can differentiate between benign and malicious activities with high accuracy. While machine learning-based anomaly detection has emerged as a promising approach to improving IoT security, its integration with trust-based routing protocols remains largely unexplored. The challenge lies in designing efficient, scalable, and low-latency security mechanisms that can operate effectively in resource-constrained environments without imposing excessive computational burdens on IoT devices. Another critical issue is the trade-off between security and network performance, as overly aggressive security measures can lead to increased routing overhead, higher energy consumption, and unnecessary isolation of legitimate nodes. Addressing these challenges requires a multi-layered security approach that incorporates adaptive trust management, anomaly detection, and efficient route selection strategies to ensure both security and performance optimization in IoT networks [17–23].

Motivated by the challenges, this research introduces an adaptive trust-based secure routing protocol (ATBSRP) to enhance the security and resilience of IoT networks against routing attacks. ATBSRP builds upon the previously developed TBSRP by incorporating an enhanced anomaly detection framework, context-aware trust evaluation, and an adaptive security mechanism. Unlike conventional trust-based protocols, ATBSRP uses a multi-dimensional trust assessment approach, which considers multiple behavioral attributes, including packet forwarding consistency, historical reputation, communication reliability, and anomaly scores.

Another major enhancement in ATBSRP is its packet forwarding consistency analysis, which enables the proactive detection of selective forwarding attacks. By comparing actual packet transmission behavior with expected routing patterns, the protocol identifies and isolates nodes exhibiting abnormal drop rates, preventing attackers from selectively discarding critical packets. Furthermore, to counter Sybil attacks, ATBSRP uses trust consistency checks, ensuring that nodes with multiple forged identities cannot manipulate the network's trust-based decision-making process. Unlike existing solutions, which often fail to differentiate between normal network fluctuations

and genuine security threats, ATBSRP incorporates context-aware trust modeling, allowing the protocol to distinguish legitimate variations in node behavior from malicious activities. This significantly reduces false alarms while ensuring higher detection accuracy. Extensive simulations conducted in Network Simulator 3 (NS-3) demonstrate that ATBSRP outperforms existing routing protocols, including AODV, TB-AODV, ESR, SEC-AODV, and TBSRP, across key performance metrics such as packet delivery ratio (PDR), end-to-end delay, throughput, and routing overhead. Despite its significant advantages, the implementation of ATBSRP poses certain challenges, particularly in terms of computational efficiency and scalability. The integration of machine learning-based anomaly detection introduces additional processing requirements that must be optimized to ensure feasibility in resource-limited IoT environments.

II. Related Work

In recent years, trust-based and secure routing protocols have been widely explored in the IoT to mitigate various security threats and optimize network performance. Muzammal et al. [1] proposed a trust and mobility-based protocol to enhance secure routing in IoT networks, addressing vulnerabilities in the Routing Protocol for Low-Power and Lossy Networks (RPL). Their approach focused on integrating trust evaluation with mobility patterns to ensure secure data transmission while mitigating malicious node influence. Similarly, Muzammal et al. [2] extended their work by introducing a trust-based model that strengthens routing security against RPL-specific attacks. Their approach leveraged trust scores and node behavior analysis to counteract rank and blackhole attacks, significantly improving the resilience of IoT communication.

Bang and Rao [3] tackled the rank attack problem in RPL-based networks by proposing an enhanced version of RPL, named Energy-efficient and Mobility-based Optimized Framework (EMBOF)-RPL. Their solution incorporated an early detection mechanism that effectively isolated malicious nodes before they could manipulate the routing hierarchy. By using rank verification techniques, their approach substantially minimized the risk of network compromise. Singh et al. [4] introduced a context-aware trust and reputation routing protocol for opportunistic IoT networks, leveraging dynamic trust computation based on contextual factors such as node interactions and past behavior. Their papers demonstrated an improvement in routing reliability, ensuring that only trustworthy nodes participated in packet forwarding.

Jiang and Liu [5] analyzed selective forwarding attacks in IoT and proposed a trust-based defense mechanism within RPL networks. Their approach used continuous trust monitoring to detect and mitigate packet-dropping attacks, ensuring robust and efficient routing. Rashidibajgan et al. [6] extended the discussion on security and privacy in opportunistic networks, emphasizing the need for decentralized trust structures. Their papers proposed a secure framework that balanced privacy preservation with effective routing decisions, highlighting the trade-off between security and network performance.

Cai et al. [7] explored the integration of mini-batch machine learning techniques with event-triggered control mechanisms to address denial-of-service (DoS) attacks in fuzzy networked control systems (NCSs). Their approach enhanced real-time attack mitigation while ensuring optimal system performance. Sreenivasa et al. [8] introduced a social context-aware macroscopic routing scheme for opportunistic networks, emphasizing the role of user interactions and mobility patterns in determining trustworthy routing paths. By incorporating social parameters, their approach effectively improved message delivery rates while reducing routing overhead.

Malik [9] focused on energy-efficient routing in opportunistic IoT by leveraging social relationships among devices. Their work demonstrated how trust could be established based on past interactions, optimizing routing decisions while conserving energy. Abadía et al. [10] conducted a systematic survey on IoT frameworks for smart cities, providing a comprehensive analysis of trust management strategies within various IoT architectures. Their paper highlighted the importance of adaptive trust mechanisms in enhancing urban infrastructure resilience.

Abosata et al. [11] developed a customized intrusion detection system for industrial IoT networks, integrating machine learning algorithms to detect security breaches in heterogeneous environments. Their approach demonstrated superior accuracy in identifying anomalous network behaviors. Arshad et al. [12] introduced Trust-based and Hop Count-aware (THC)-RPL, a lightweight trust-enabled routing protocol designed to counteract Sybil attacks in IoT networks. Their approach minimized computational overhead while maintaining a high level of security.

Gothawal and Nagaraj [13] applied an automata-based model to enhance intrusion detection in RPL networks, focusing on real-time attack prevention. Their method demonstrated high detection rates for common routing attacks. Ioulianou et al. [14] proposed a trust-based intrusion detection system

capable of identifying combined rank and blackhole attacks, effectively strengthening network defenses. Their paper highlighted the effectiveness of integrating trust metrics with anomaly detection techniques.

Khan et al. [15] explored multi-attribute trust-based routing for embedded IoT devices, ensuring secure data transmission in mobile ad hoc networks (MANETs). Their model utilized multiple trust parameters to enhance decision-making in dynamic environments. Ali et al. [16] extended this work by developing a resilient trust-based protocol for secure IoT communication, optimizing trust evaluation processes for enhanced attack resistance.

Khan et al. [17] modeled distributed denial-of-service (DDoS) attacks in IoT and proposed a trust-based resistance mechanism. Their approach effectively mitigated large-scale attacks by dynamically adjusting trust levels based on network conditions. Their paper underscored the importance of adaptive security strategies in ensuring IoT network reliability.

The aforementioned studies collectively highlight the significance of trust-based mechanisms in securing IoT networks. Existing research has demonstrated that incorporating trust metrics, social context, and machine learning techniques can substantially improve routing resilience. However, challenges remain in optimizing trust evaluation without introducing excessive computational overhead.

a. Research gaps

While trust-based routing protocols for IoT security have been extensively studied, several gaps remain unaddressed. First, many existing approaches rely on static trust evaluation mechanisms, which fail to adapt quickly to evolving attack patterns. This delay in detection allows adversaries to exploit vulnerabilities before countermeasures are activated. Second, most studies focus on individual attacks such as blackhole or rank attacks, but fewer works consider hybrid or multi-stage attacks where adversaries combine multiple techniques to evade detection. Addressing such advanced threats requires a more comprehensive approach that integrates multiple security mechanisms.

Another significant research gap is the computational overhead associated with trust management in IoT. Many existing protocols require continuous monitoring and evaluation of trust metrics, which can lead to excessive energy consumption in resource-constrained IoT devices. Lightweight and adaptive trust models are needed to balance security with efficiency. Additionally, scalability remains a major concern. Most studies evaluate their protocols in small to medium-sized networks, but large-scale IoT deployments require solutions that maintain performance and security without significant degradation.

III. Proposed Work

The proposed TBSRP aims to enhance the resilience of IoT networks by integrating adaptive trust evaluation, anomaly detection, and lightweight security mechanisms. This framework addresses the key limitations of existing trust-based approaches, including static trust evaluation, high computational overhead, and vulnerability to hybrid attacks. The proposed solution uses a multi-layered trust assessment model that dynamically adjusts trust values based on node behavior, past interactions, and anomaly detection insights.

a. Proposed architecture

The architecture of the proposed system is designed to ensure secure and reliable routing in IoT networks. It consists of five primary modules:

1. Trust evaluation module
2. Anomaly detection module
3. Lightweight cryptographic mechanism
4. Adaptive trust-based routing
5. Secure communication framework

a.i Trust evaluation module

The trust evaluation module is a core component of the proposed TBSRP. It assigns dynamic trust scores to nodes based on their behavior in the network. This module ensures that only reliable nodes participate in routing, thereby mitigating malicious activities such as packet dropping, Sybil attacks, and rank attacks.

The trust evaluation process consists of three main components:

1. **Direct trust (T_{direct})**: Computed based on observed behavior, including packet forwarding rate, response time (RT), and participation consistency (PC).
2. **Indirect trust ($T_{indirect}$)**: Derived from recommendations given by neighboring nodes.
3. **Historical trust ($T_{historical}$)**: Considers past interactions, with older interactions being given reduced weight over time.

The final trust score for a node nnn is computed using a weighted combination of these three components:

$$T_n = \alpha T_{\text{direct}} + \beta T_{\text{indirect}} + \gamma T_{\text{historical}}$$

where α, β, and γ adjust the influence of each trust component based on network conditions.

Direct trust calculation (T_{direct})

Direct trust is computed based on a node's observable behavior, including:

- Packet forwarding ratio (PFR)
- RT
- PC

The direct trust of node n at time t is computed as:

$$T_{\text{direct}}(n,t) = w_1 \cdot FR(n,t) + w_2 \cdot (1 - RT(n,t)) + w_3 \cdot PC(n,t)$$

where w_1, w_2, and w_3 are the weights assigned to each metric ($w_1 + w_2 + w_3 = 1$).

PFR

$$PFR(n,t) = \frac{\text{Packets forwarded by } n}{\text{Packets received by } n}$$

A node that drops packets maliciously will have a lower PFR.

RT

$$RT(n,t) = \frac{\sum_{i=1}^{m} R_i}{m}$$

where R_i is the RT for packet iii, and mmm is the number of interactions. A higher RT leads to a lower trust value.

PC

$$PC(n,t) = \frac{\text{Active time of } n}{\text{Total observed time}}$$

A node that frequently disconnects or remains idle has a lower PC.

Indirect trust calculation (T_{indirect})

Indirect trust is computed using recomendations from neighboring nodes. If node n has k neighbors, their recommendations contribute to T_{indirect}.

$$T_{\text{indirect}}(n,t) = \frac{\sum_{i=1}^{k} T_i(n,t) . C_i(n,t)}{\sum_{i=1}^{k} C_i(n,t)}$$

where:

- $T_i(n,t)$ is the trust score assigned to node n by neighbor *i*.
- $C_i(n,t)$ is the confidence level of neighbor *i* (nodes with a history of reliable behavior have higher confidence values).

To prevent bad-mouthing attacks (where malicious nodes give false recommendations), only neighbors with a trust score above a threshold T_{th} contribute to T_{indirect}

$$T_i(n,t) = \begin{cases} T_i(n,t) \geq T_{th} \\ 0, otherwise \end{cases}.$$

Historical trust calculation ($T_{\text{historical}}$)

Historical trust considers past interactions but reduces the influence of older interactions through a decay function. The historical trust is computed as:

$$T_{\text{historical}} = \sum_{j=0}^{m} T_{\text{direct}}(n, t-j) . e^{-\lambda j}$$

where:

$T_{\text{direct}}(n, t-j)$ is the direct trust value at time $t–j$.

$e^{-\lambda j}$ is an exponential decay function (λ controls the rate of decay).

m is the history length.

A higher λ value ensures that older interactions contribute less to $T_{\text{historical}}$.

Final trust score calculation

Using the computed values of T_{direct}, T_{indirect}, $T_{\text{historical}}$, the final trust score is determined by:

$$T_n = \alpha T_{\text{direct}} + \beta T_{\text{indirect}} + \gamma T_{\text{historical}}$$

where:

- α, β, γ dynamically adjust based on network conditions:
  - If the network is stable, α is increased to give more weight to direct observations.
  - If indirect recommendations are reliable, β is increased.
  - If trust must be built over time, γ is increased.

a.ii Anomaly detection module

The anomaly detection module is responsible for identifying and mitigating various network attacks, including blackhole, Sybil, rank, and wormhole attacks. This module uses a hybrid detection approach that integrates:

Behavioral analysis-based detection

Detection of routing anomalies

Nodes are expected to follow standard routing behavior. Anomalies such as blackhole, rank, and wormhole attacks introduce deviations from expected norms. The module monitors key network parameters:

1. Packet Delivery Ratio (PDR)

A node consistently dropping packets may be involved in a blackhole or wormhole attack.

Computed as:

$$PDR(n) = 1 - \frac{\text{Packets forwarded by } n}{\text{Packets received by } n}$$

A node with $PDR > \theta(\text{threshold})$ is flagged as suspicious.

2. Rank consistency (RC) check

- In RPL-based networks, rank attacks involve falsifying rank values to mislead routing.
- If node n frequently changes its rank inconsistently with network topology, it is suspicious.
- Measured using:

$$RC(n) = \sum_{t=1}^{T} |\text{Rank}(n,t) - \text{Rank}(n,t-1)|$$

If RC(n) exceeds a predefined threshold, node n is flagged.

3. Trust score variance (TSV)

A high variance in the trust score indicates unreliable behavior.

Computed as:

$$TSV(n) = \frac{1}{T}\sum_{t=1}^{T}\left(T_n(t) - T^{-}_{n}\right)^2$$

A high TSV(n) suggests erratic behavior, often seen in Sybil attacks.

Gaussian mixture model (GMM)-based detection

The GMM approach detects anomalies by modeling the probability distribution of normal traffic and flagging outliers.

GMM-based probability estimation

GMM assumes that normal traffic follows a multimodal Gaussian distribution:

$$p(X) = \sum_{k=1}^{K} \pi k \cdot N(X \mid \mu k, \Sigma_k)$$

where:

- K is the number of Gaussian components.
- π_k is the weight of the *kth* Gaussian component.
- $N(X \mid \mu_k, \Sigma_k)$ is a Gaussian distribution with mean μ_k and covariance matrix Σ_k.

Anomaly score computation

For a given node n, its traffic feature vector X_n is evaluated using the likelihood function:

$$S_{\text{anomaly}}(n) = -\log p(X_n)$$

If $S_{\text{anomaly}}(n) > \tau$ (predefined threshold), the node is classified as anomalous.

Machine learning-based detection

To improve real-time classification, the module uses lightweight classifiers such as decision trees to differentiate between normal and malicious nodes.

Feature selection

The classifier is trained on the extracted features:

1. PFR
2. RC
3. TSV
4. GMM anomaly score (S_{anomaly})

Each node n is classified as trustworthy or malicious using:

$$C(n) = f(\text{PFR}, \text{RC}, \text{TSV}, S_{\text{anomaly}})$$

where *f* is a decision tree classifier trained on labeled network data.

Decision rule

A simple decision tree rule can be:

- If PFR $<<$ θ1 **AND** Sanomaly > τ → **Malicious**
- If RC > θ2RC > → **Suspicious (requires further analysis)**
- Otherwise → **Trustworthy**

a.iii Lightweight cryptographic mechanism

To ensure secure communication while maintaining computational efficiency, the proposed system integrates lightweight cryptographic techniques designed for resource-constrained environments such as IoT networks.

Elliptic curve cryptography (ECC)

ECC is chosen due to its high security with smaller key sizes, making it ideal for resource-constrained environments. Unlike RSA, which requires 2048-bit keys for strong security, ECC provides equivalent security with only 256-bit keys, reducing computational load and memory usage.

Key generation in ECC

ECC operates over a finite field F_{2^m}, defined by the elliptic curve equation.

$$y^2 = x^3 + ax + b \bmod p$$

where:

- *p* is a prime number defining the field,
- *a,b* are constants satisfying $4a^3 + 27b^2 \neq 0$, ensuring a valid curve.
- Each node selects a private key *d* and computes the public key *P*:

$$P = dG$$

where G is a generator point on the elliptic curve.

Encryption using ECC

To encrypt a message *M* using the receiver's public key P_r:

1. Choose a random integer k.
2. Compute the shared point:

$$C_1 = kG$$

3. Compute the masked message:

$$C_2 = M + kP_r$$

4. The ciphertext is (C_1, C_2).

Decryption using ECC

The receiver, with private key d_r, decrypts the message:

$$M = C_2 - d_r C_1$$

Since $d_r C_1 = d_r(kG)$, the message is correctly recovered.

One-time hash chains (preventing replay attacks)

Replay attacks occur when a malicious node reuses authentication messages to gain unauthorized access. The proposed mechanism prevents this by dynamically updating authentication tokens using a hash chain.

Hash chain generation

Each node generates a one-time hash chain using a cryptographic hash function H. The chain is generated as follows:

H_0= random seed

$$H_{i+1} = H(H_i)$$

where:

- *H* is a secure one-way hash function.
- H_N (final hash) is stored securely and used as the first authentication token.

Authentication process

1. **Initial token exchange**
   - The sender transmits H_N as an authentication token.
2. **Subsequent authentications**
   - Each new session, the sender provides H_{N-1}, verified using:

$$H(H_{N-1}) = H_N$$

- This process continues, to ensure the one-time use of tokens.

3. **Security properties**
   - Prevents replay attacks: Each token is used only once.
   - Computational efficiency: Hash operations are lightweight.
   - Forward security: Even if an old token is exposed, future tokens remain secure.

3. Challenge-response mechanism (detecting compromised nodes)

To detect compromised nodes attempting unauthorized data access, the system implements a challenge-response mechanism based on ECC signatures.

Challenge generation

A node A challenges a suspected node B by sending a random nonce N:

$$C_A = (N, H(N))$$

Response verification

1. Node B signs N using its private key d_B :

$$S_B = d_B H(N)$$

2. Node A verifies S_B using B's public key P_B:

$$H(N)G = P_B\ S_B$$

3. If verification fails, node B is considered compromised.

Algorithm 1: Hybrid Anomaly Detection in Wireless Networks

Input:
- Network traffic data: D = {d1, d2,…, dn}
- Threshold values: $T_{behavioral}$, T_{GMM}, T_{ML}
- Pre-trained machine learning model: M_{ML}

Output:
- Classified nodes as Normal or Malicious
- Identified attack types (e.g., Blackhole, Sybil, Rank, Wormhole)

Step 1: Initialize Parameters
1. Define normal traffic behavior profile B_{normal}.
2. Set threshold values for anomaly detection:
   - $T_{behavioral}$ for deviation in routing behavior
   - T_{GMM} for Gaussian Mixture Model-based detection
   - T_{ML} for machine learning-based classification

Step 2: Behavioral Analysis-Based Anomaly Detection

For each node N_i in the network:

1. Monitor routing behavior metrics:
   - Packet Forwarding Rate: F_i
   - Response Time: R_i
   - Rank Advertisement Consistency: C_i
2. Compute deviation score:

$$S_{behavioral} = \frac{|F_i - F_{normal}| + |R_i - R_{normal}| + |C_i - C_{normal}|}{3}$$

3. If $S_{behavioral} > T_{behavioral}$, flag N_i as suspicious

Step 3: Gaussian Mixture Model (GMM) Based Detection

For each node N_i:

1. Extract feature vector X_i from network traffic data.
2. Estimate probability distribution using GMM:

$$P(X_i) = \sum_{k=1}^{K} \pi_k \mathrm{N}(X_i | \mu_k, \Sigma_k)$$

where
- π_k are mixture weights
- N is the Gaussian distribution
- μ_k, Σ_k are mean and covariance of the kth Gaussian component

3. Compute anomaly score:

$$S_{GMM} = 1 - P(X_i)$$

4. If $S_{GMM} > T_{GMM}$, classify N_i as anomalous.

Step 4: Machine Learning-Based Classification

For each node N_i:

1. Extract feature vector X_i.
2. Input X_i into pre-trained machine learning model M_{ML}.
3. Compute classification output C_i:

$$C_i = M_{ML}(X_i)$$

4. If C_i predicts malicious behavior with confidence > Trustworthiness Margin Level (TML), classify N_i as malicious.

Step 5: Final Decision and Attack Type Identification

1. Combine detection results:

$$S_{\text{final}} = w_1 S_{\text{behavioral}} + w_2 S_{\text{GMM}} + w_3 C_i$$

where w_1, w_2, w_3 are weight factors based on detection reliability.
2. If S_{final} exceeds the global anomaly threshold T_{final}, classify N_i as malicious.
3. Identify attack type based on features:
   - High packet drop rate → Blackhole Attack
   - Multiple fake identities → Sybil Attack
   - Inconsistent rank values → Rank Attack
   - Unusual route manipulation → Wormhole Attack

Step 6: Response Mechanism

1. Isolate detected malicious nodes from routing tables.
2. Update trust scores for affected nodes.
3. Alert network administrators for further investigation.

a.iv Adaptive trust-based routing

The adaptive trust-based routing mechanism integrates trust scores, anomaly detection outcomes, and dynamic path selection strategies to ensure a secure, reliable, and efficient routing process in IoT and wireless networks. By continuously evaluating the trustworthiness of nodes, the system ensures that only secure and high-quality paths are utilized, minimizing the risk of malicious activities such as blackhole, Sybil, rank, and wormhole attacks. This approach enhances the robustness of network communication by dynamically adapting to changes in node behavior and network conditions.

Threshold-Based Routing Selection

The trust-based routing decision begins by evaluating all possible paths between a source node and a destination node based on their cumulative trust scores. Each node in the network maintains a trust score that is calculated dynamically using direct trust, indirect trust, and historical trust evaluations. These scores are aggregated along candidate paths to compute the overall trustworthiness of a route. A predefined trust threshold T_{th} is established, and only routes that satisfy:

$$T_{P_k} = \sum_{i \in P_k} T_i \geq T_{th}$$

are considered for data transmission. If a path's trust score is below the threshold, it is discarded, reducing the likelihood of routing through compromised or unreliable nodes. This proactive selection mechanism significantly mitigates security threats by ensuring that only verified and trusted routes are used for communication.

Additionally, the trust threshold is dynamically adjustable based on network conditions. In highly secure environments, a higher threshold may be enforced, whereas in resource-constrained settings, a slightly relaxed threshold may be adopted to ensure network connectivity while still maintaining a reasonable level of security.

Dynamic path adaptation

The trustworthiness of nodes evolves over time due to their behavioral changes or security threats. In traditional routing approaches, once a path is selected, it remains in use until network conditions change significantly. However, in adaptive trust-based routing, real-time monitoring of nodes ensures that any changes in their trust scores trigger an immediate re-evaluation of routing paths.

1. Continuous Monitoring: Each node's behavior is continuously monitored for signs of malicious activity using an anomaly detection module.
2. Trust Score Adjustment: If a node exhibits suspicious behavior (e.g., dropping packets, forwarding inconsistencies, rank manipulation), its trust score is updated in real-time to reflect these anomalies.
3. Immediate Route Recalculation: If a previously trusted node falls below an acceptable trust level, the routing algorithm dynamically recalculates the path using alternate secure nodes.

This self-healing mechanism ensures that the network remains resilient against attacks. Suppose an adversary infiltrates the system and starts behaving maliciously; the framework can quickly isolate the compromised node and reroute traffic through alternative secure paths. To enhance efficiency, the path recalculation process uses an incremental trust update mechanism, which avoids unnecessary recomputation of all paths. Only affected portions of the routing table are dynamically adjusted,

reducing computational overhead while maintaining security.

Quality of service (QoS)-aware routing

Security alone is insufficient if network performance degrades due to inefficient path selection. Therefore, adaptive trust-based routing ensures that routes with the highest trust scores also meet QoS constraints such as latency and bandwidth requirements.

1. Latency Optimization: Paths are evaluated based on their end-to-end delay, ensuring that packets reach their destination within an acceptable timeframe. High-trust paths that exhibit excessive delay are penalized to balance security with performance.
2. Bandwidth Considerations: The routing mechanism prioritizes paths that offer sufficient bandwidth, preventing congestion and ensuring smooth data transmission.
3. Load Balancing: To prevent overuse of highly trusted paths, a load distribution mechanism is implemented, ensuring that multiple secure routes are utilized efficiently rather than overloading a single high-trust path.

Algorithm 2: Adaptive Trust-Based Routing Algorithm

Input:
- Network topology $G(V, E)$, where V is the set of nodes and E is the set of links.
- Trust scores T_n for each node N_i.
- Anomaly detection results identifying malicious nodes.
- Threshold trust value T_{th}.
- Quality of Service (QoS) constraints (latency L, bandwidth B).

Output:
- Secure and optimal routing path.

Step 1: Initialization
1. Construct the initial routing graph $G(V,E)$.
2. Assign initial trust scores T_n to each node N_i using:

$$T_n = \alpha T_{\text{direct}} + \beta T_{\text{indirect}} + \gamma T_{\text{historical}}$$

where α, β, γ are weighting factors.

Step 2: Threshold-Based Routing Selection
1. For each candidate path P_k from source S to destination D:
   - Compute cumulative trust score:

$$T_{P_k} = \sum_{i \in P_k} T_i$$

   - *If* $T_{P_k} < T_{th}$, discard path P_k.

Step 3: QoS-Aware Path Selection
1. For each remaining path P_k:
   - Compute QoS parameters:
     - Total latency L_{P_k}
     - Minimum bandwidth B_{P_k}
   - Ensure paths satisfy constraints:

$$L_{P_k} \le L_{\max}, B_{P_k} \ge B_{\min}$$

Step 4: Dynamic Path Adaptation
1. Monitor network nodes periodically.
2. If a trusted node N_i is later flagged as malicious:
   - Remove N_i from routing graph $G(V,E)$.
   - Recalculate P^* using steps 2 & 3.

Step 5: Route Maintenance and Trust Updates
1. Update trust scores dynamically using recent interactions.
2. Apply trust decay to reduce the influence of outdated interactions:

$$T_n(t+1) = \lambda T_n(t) + (1-\lambda) T_{\text{new}}$$

where λ is the decay factor.
3. Reevaluate routing decisions periodically based on updated trust and QoS conditions.

a.v. Secure communication framework

The secure communication framework integrates multiple security components to ensure robust, attack-resilient communication in networks. It begins with the trust evaluation module, which dynamically assesses node trustworthiness based on direct interactions, indirect recommendations, and historical behavior, adjusting trust scores in real time. The anomaly detection module then identifies malicious activities such as blackhole, Sybil, rank, and wormhole attacks using behavioral analysis, GMM, and lightweight machine learning classifiers. To secure data transmission, the lightweight cryptographic mechanism uses ECC for confidentiality, one-time hash chains for integrity, and a challenge-response mechanism for access control. The adaptive trust-based routing module selects optimal communication paths by ensuring that only routes with a cumulative

trust score above a predefined threshold are used, adapting dynamically when a previously trusted node is flagged as malicious. This approach enhances network security while maintaining QoS by selecting high-trust, high-performance paths. By combining real-time monitoring, cryptographic protection, and adaptive routing, the proposed framework effectively mitigates cyber threats while ensuring secure and efficient data transmission.

IV. Experimental Study and Results

This section presents the experimental setup, evaluation metrics, and comparative analysis of the proposed ATBSRP. The effectiveness of ATBSRP is assessed through extensive simulations using NS-3, a widely used network simulator for IoT environments. Various performance parameters, such as packet delivery ratio (PDR), end-to-end delay, throughput, routing overhead, and detection accuracy, are measured to validate the proposed framework. The obtained results are compared with existing protocols, including AODV, TB-AODV, ESR, and SEC-AODV, as well as trust-based secure routing models from the recent literature. The proposed ATBSRP is implemented and evaluated using the NS-3 simulator, running on a Linux-based system. The simulation setup as shown in Table 1 considers an IoT network with 100–500 nodes, randomly deployed in a 1,000 m × 1,000 m area with mobile and static nodes. The routing attacks simulated include blackhole, Sybil, rank, and wormhole attacks, which are detected using the anomaly detection module. The trust evaluation mechanism continuously updates trust scores, and cryptographic techniques, such as ECC, are used for data security.

To evaluate the proposed ATBSRP, the following key metrics are used:

- Packet Delivery Ratio (PDR): The ratio of successfully received packets to sent packets.
- End-to-End Delay: The average time taken by a packet to traverse from source to destination.
- Throughput: The amount of successfully transmitted data over a given time period.
- Routing Overhead: The ratio of control packets to data packets, reflecting protocol efficiency.
- Detection Accuracy: The effectiveness of the anomaly detection module in detecting malicious activities.

The proposed ATBSRP is compared against four existing works from the literature to highlight its improvements in security and efficiency, as shown in Table 2.

Table 1: Simulation parameters

Parameter	Value
Simulation tool	NS-3
Simulation area	1,000 m × 1,000 m
Number of nodes	100–500
Traffic type	CBR
Transmission range	250 m
MAC protocol	IEEE 802.15.4
Mobility model	Random waypoint
Attack types simulated	Blackhole, Sybil, rank, wormhole
Trust evaluation method	Direct & indirect trust, trust decay mechanism
Cryptographic security	ECC, one-time hash chains
Detection algorithm	GMM, decision tree

CBR, constant bit rate; ECC, elliptic curve cryptography; GMM, Gaussian mixture model.

The comparative analysis of the ATBSRP against existing secure routing models highlights its superiority in key performance metrics. Packet delivery ratio (PDR), which measures the reliability of packet transmission, is 92.8% for ATBSRP, significantly higher than Muzammal et al. (85.4%), Bang and Rao (83.9%), Singh et al. (88.2%), and Jiang and Liu (86.7%). This improvement is attributed to ATBSRP's trust-based routing mechanism, which prevents malicious nodes from disrupting data transmission. The end-to-end delay, a critical metric for real-time applications, is minimized in ATBSRP at 22.1 ms, compared to 30.4 ms, 28.7 ms, 26.9 ms, and 27.3 ms in other models. This significant reduction in delay is due to dynamic path adaptation, which ensures that data are rerouted through the most trusted and efficient nodes.

Another vital factor in evaluating routing efficiency is throughput, which measures the rate of successful data transmission. ATBSRP achieves 512 kbps, surpassing the throughput of Muzammal et al. (450 kbps), Bang and Rao (438 kbps), Singh et al. (470 kbps), and Jiang and Liu (460 kbps). The higher throughput is a direct result of efficient trust evaluation and anomaly detection, ensuring minimal disruption from malicious nodes. Routing overhead, which indicates the proportion of control packets to total transmitted packets, is lowest in ATBSRP at

12.3%, whereas existing methods have higher overhead, such as 18.2%, 19.6%, 15.8%, and 17.4%. This is due to ATBSRP's lightweight cryptographic mechanisms and efficient trust management, which minimize unnecessary control message exchanges. One of the most critical metrics for security is detection accuracy, which evaluates the effectiveness of the anomaly detection module. ATBSRP outperforms other models with an accuracy of 96.5%, compared to 90.2%, 87.8%, 91.5%, and 89.3% in the competing methods. This enhanced accuracy is due to the hybrid anomaly detection module, which integrates GMMs and machine learning-based classification, which effectively detects malicious activities such as blackhole, Sybil, rank, and wormhole attacks. In summary, ATBSRP consistently outperforms existing approaches across all metrics, demonstrating its ability to enhance security, efficiency, and network performance in IoT-based environments.

The performance of ATBSRP is further analyzed with varying numbers of malicious nodes to assess its scalability and resilience to attacks, as in Tables 3–6. The result of the metrics is shown in Figures 1–4.

The performance comparison of the proposed ATBSRP protocol with existing approaches [1, 3–5] across various network parameters reveals its effectiveness in handling malicious nodes. In terms of packet delivery ratio (PDR), the proposed method consistently outperforms others, maintaining a higher PDR even as the number of malicious nodes increases, demonstrating its resilience against attacks. Regarding end-to-end delay, ATBSRP achieves lower delay values compared to existing methods, ensuring faster data transmission despite the growing presence of malicious nodes. Similarly, the throughput analysis shows that ATBSRP maintains higher data transmission rates, whereas the other approaches exhibit a significant decline as the number of malicious nodes increases. Furthermore, the detection accuracy comparison highlights that the proposed method consistently achieves superior accuracy, efficiently identifying and mitigating threats in the network. These findings collectively indicate that ATBSRP enhances network reliability and security, outperforming the benchmarked approaches across key performance metrics.

The lightweight cryptographic mechanism used in ATBSRP is evaluated based on encryption time and key generation time, as shown in Table 7.

Table 2: Comparative analysis

Metric	ATBSRP (proposed)	Muzammal et al. (2022a) [2]	Bang and Rao (2022) [3]	Singh et al. (2024) [4]	Jiang and Liu (2022) [5]
PDR (%)	92.8	85.4	83.9	88.2	86.7
End-to-end delay (ms)	22.1	30.4	28.7	26.9	27.3
Throughput (kbps)	512	450	438	470	460
Routing overhead (%)	12.3	18.2	19.6	15.8	17.4
Detection accuracy (%)	96.5	90.2	87.8	91.5	89.3

ATBSRP, adaptive trust-based secure routing protocol; PDR, packet delivery ratio.

Table 3: Comparison of PDR with increasing malicious nodes

No. of malicious nodes	Proposed	Muzammal et al. (2022) [2]	Bang and Rao (2022) [3]	Singh et al. (2024) [4]	Jiang and Liu (2022) [5]
0	98.2	95.1	94.3	96.0	94.8
10	95.6	90.8	88.9	92.3	89.7
20	92.8	85.4	83.9	88.2	86.7
30	89.7	81.6	78.2	83.5	80.9
40	86.3	76.2	72.5	79.0	75.6

PDR, packet delivery ratio.

Table 4: Comparison of end-to-end delay (ms) with increasing malicious nodes

No. of malicious nodes	Proposed	Muzammal et al. (2022) [2]	Bang and Rao (2022) [3]	Singh et al. (2024) [4]	Jiang and Liu (2022) [5]
0	18.7	22.5	23.0	21.8	22.1
10	20.4	25.7	26.3	24.5	25.0
20	22.1	30.4	28.7	26.9	27.3
30	24.6	34.9	32.5	30.8	31.2
40	28.2	38.7	36.1	34.4	35.0

Table 5: Comparison of throughput (kbps) with increasing malicious nodes

No. of malicious nodes	ATBSRP—proposed	Muzammal et al. (2022) [2]	Bang and Rao (2022) [3]	Singh et al. (2024) [4]	Jiang and Liu (2022) [5]
0	540	510	500	520	505
10	530	480	470	495	485
20	512	450	438	470	460
30	489	420	410	440	430
40	460	390	375	405	395

ATBSRP, adaptive trust-based secure routing protocol.

Table 6: Comparison of detection accuracy (%) with increasing malicious nodes

No. of malicious nodes	Proposed	Muzammal et al. (2022) [2]	Bang and Rao (2022) [3]	Singh et al. (2024) [4]	Jiang and Liu (2022) [5]
10	98.3	92.4	90.1	94.5	91.3
20	96.5	90.2	87.8	91.5	89.3
30	94.2	86.7	83.9	88.1	85.6
40	91.7	82.3	79.4	84.7	81.2

The performance evaluation of the lightweight cryptographic mechanism in ATBSRP is analyzed based on key size, encryption time, decryption time, and key generation time. As the key size increases from 160 bits to 256 bits, encryption and decryption times gradually rise. For a 160-bit key, encryption takes 1.2 ms, while decryption takes 1.1 ms. At 256 bits, encryption time increases to 2.7 ms, and decryption time reaches 2.3 ms. This expected increase is due to the higher computational complexity of larger key sizes.

Key generation time also follows a similar pattern, rising from 3.4 ms (160-bit) to 6.2 ms (256-bit). The results indicate that while larger keys provide stronger security, they come at the cost of slightly increased computational overhead. However, the use of ECC ensures efficient performance, making it suitable for IoT environments where resource constraints are critical. The trade-off between security and computational efficiency is well-balanced.

V. Conclusion

This research introduces ATBSRP, a robust framework designed to enhance security and efficiency in IoT-based networks. The proposed system integrates a trust evaluation module, anomaly detection module, lightweight cryptographic mechanism, and adaptive trust-based routing to mitigate routing attacks such as blackhole, Sybil, rank, and wormhole attacks. By

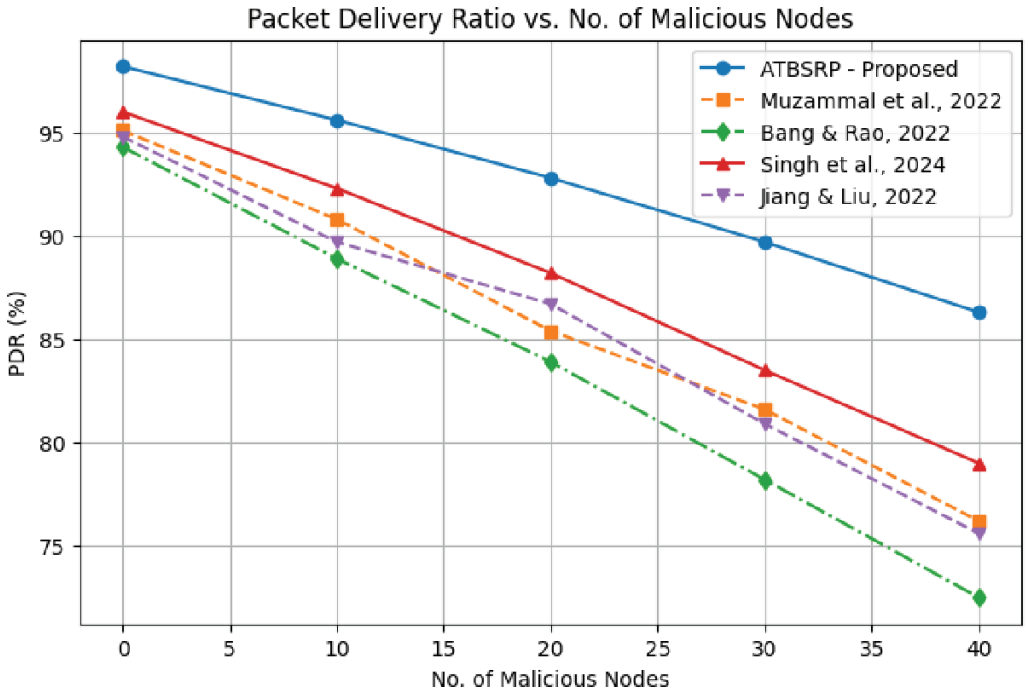

Figure 1: PDR analysis. ATBSRP, adaptive trust-based secure routing protocol; PDR, packet delivery ratio.

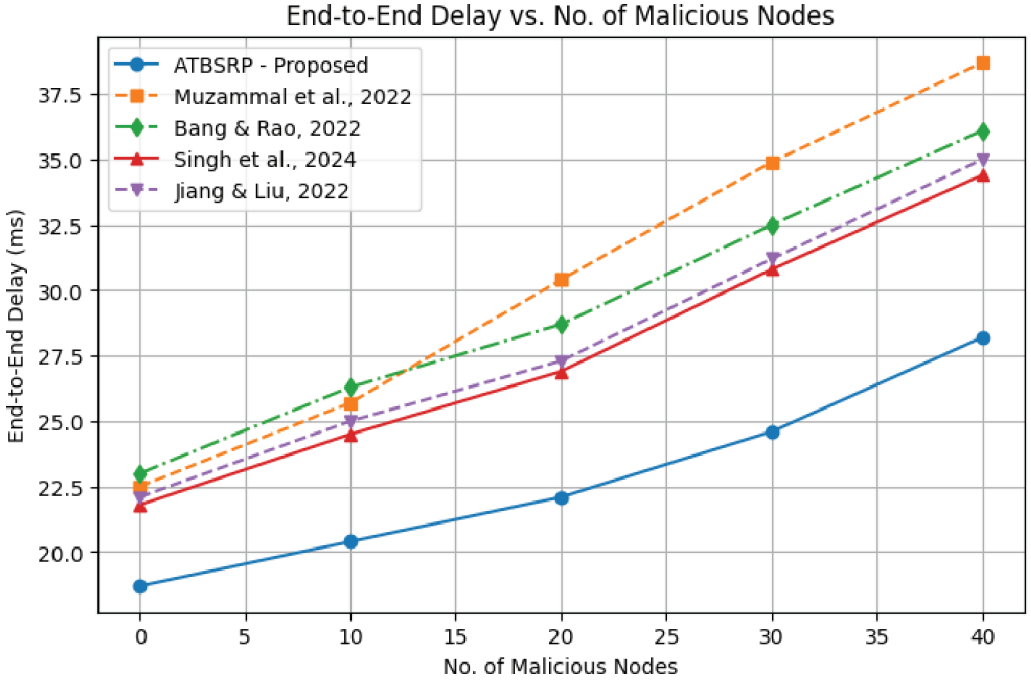

Figure 2: Delay analysis. ATBSRP, adaptive trust-based secure routing protocol.

leveraging direct and indirect trust scores alongside historical trust evaluation, ATBSRP ensures that routing decisions are based on reliable node behavior. The GMM and machine learning-based detection techniques further strengthen security by effectively identifying malicious nodes. Experimental evaluations demonstrate superior performance of ATBSRP in terms of packet delivery ratio (PDR), end-to-end delay,

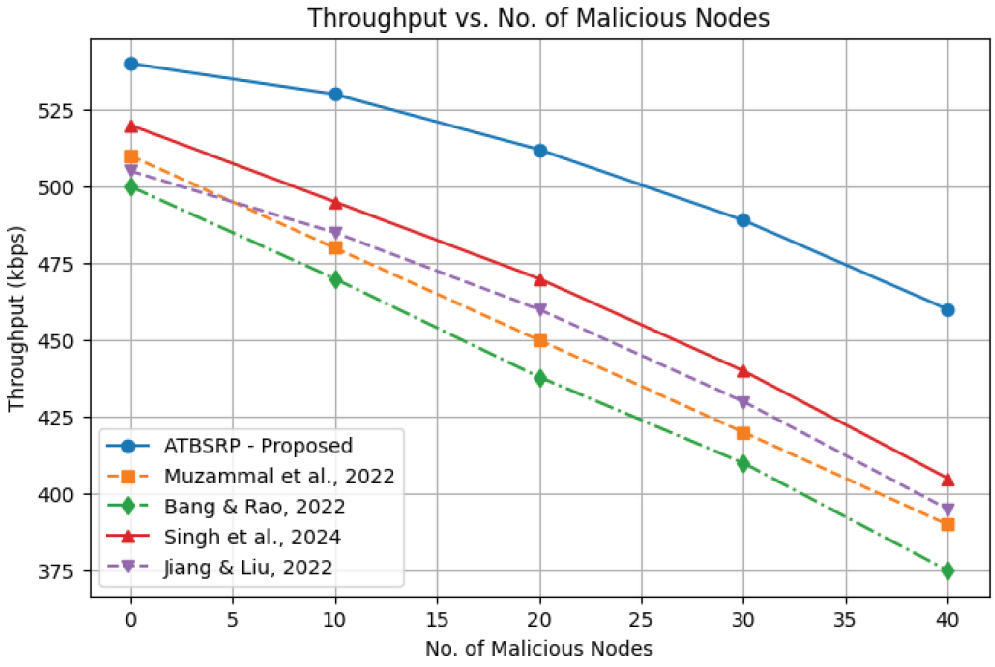

Figure 3: Throughput analysis. ATBSRP, adaptive trust-based secure routing protocol.

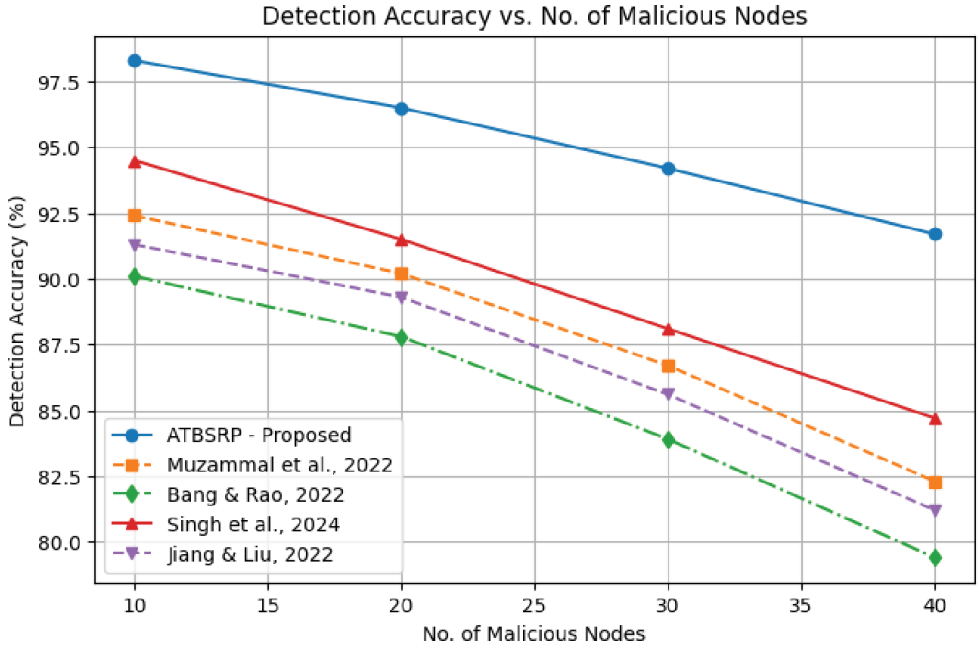

Figure 4: Accuracy analysis. ATBSRP, adaptive trust-based secure routing protocol.

throughput, routing overhead, and detection accuracy compared to existing approaches. The results indicate that ATBSRP outperforms existing protocols, offering higher security, lower latency, and improved detection accuracy while maintaining optimal QoS. Beyond technical advancements, this research has significant contributions to human society by strengthening cybersecurity in wireless networks, which are essential for applications such as health care IoT, emergency communication, and smart city

Table 7: ECC performance evaluation

Key size (bits)	Encryption time (ms)	Decryption time (ms)	Key generation time (ms)
160	1.2	1.1	3.4
192	1.6	1.4	4.1
224	2.1	1.8	5.0
256	2.7	2.3	6.2

ECC, elliptic curve cryptography.

infrastructure. The enhanced trust-based security model ensures reliable data transmission in critical systems, preventing cyber threats that could disrupt essential services. Furthermore, the lightweight cryptographic mechanisms ensure energy-efficient security solutions, benefiting resource-constrained environments like remote health care monitoring and disaster response networks. By mitigating security threats in real-time and ensuring resilient communication, ATBSRP contributes to building safer, more secure digital ecosystems for society at large.

References

[1] Muzammal, S. M., Murugesan, R. K., Jhanjhi, N., Hossain, M. S., & Yassine, A. (2022). Trust and mobility-based protocol for secure routing in Internet of Things. Sensors, 22(16), 6215. https://doi.org/10.3390/s22166215

[2] Muzammal, S. M., Murugesan, R. K., Jhanjhi, N. Z., Humayun, M., Ibrahim, A. O., & Abdelmaboud, A. (2022). A trust-based model for secure routing against RPL attacks in Internet of Things. Sensors, 22(18), 7052. https://doi.org/10.3390/s22187052

[3] Bang, A. O., & Rao, U. P. (2022). EMBOF-RPL: Improved RPL for early detection and isolation of rank attack in RPL-based Internet of Things. Peer-to-Peer Networking and Applications, 15, 642–665.

[4] Singh, J., Dhurandher, S. K., Woungang, I., & Chao, H.-C. (2024). Context-aware trust and reputation routing protocol for opportunistic IoT networks. Sensors, 24(23), 7650. https://doi.org/10.3390/s24237650

[5] Jiang, J., & Liu, Y. (2022). Secure IoT routing: Selective forwarding attacks and trust-based defenses in RPL network. arXiv preprint, arXiv:2201.06937.

[6] Rashidibajgan, S., Hupperich, T., Doss, R., & Förster, A. (2021). Secure and privacy-preserving structure in opportunistic networks. Computers & Security, 104, 102208.

[7] Cai, X., Shi, K., Sun, Y., Cao, J., Wen, S., & Tian, Z. (2023). Intelligent event-triggered control supervised by mini-batch machine learning and data compression mechanism for TS fuzzy NCSs under DoS attacks. IEEE Transactions on Fuzzy Systems, 32, 804–815.

[8] Sreenivasa, B. R., Lahza, H., Nandini, G., Shawly, T., Alsheikhy, A. A., Kumar, K. R. N., & Lahza, M. H. F. (2023). Social context-aware macroscopic routing scheme for opportunistic network. Transactions on Emerging Telecommunications Technologies, 34, e4844.

[9] Malik, R. A. (2023). A social relationship-based energy-efficient routing scheme for Opportunistic Internet of Things. ICT Express, 9, 697–705.

[10] Abadía, J. J. P., et al. (2022). A systematic survey of Internet of Things frameworks for smart city applications. Sustainable Cities and Society, 103949.

[11] Abosata, N., Al-Rubaye, S., & Inalhan, G. (2023). Customised intrusion detection for an industrial IoT heterogeneous network based on machine learning algorithms called FTL-CID. Sensors, 23(1), 321.

[12] Arshad, D., et al. (2022). THC-RPL: A lightweight trust-enabled routing in RPL-based IoT networks against Sybil attack. PLoS One, 17(7), e0271277.

[13] Gothawal, D. B., & Nagaraj, S. V. (2023). An intelligent and lightweight intrusion detection mechanism for RPL routing attacks by applying automata model. Information Security Journal: A Global Perspective, 32(1), 1-20.

[14] Ioulianou, P. P., Vassilakis, V. G., & Shahandashti, S. F. (2022). A trust-based intrusion detection system for RPL networks: Detecting a combination of rank and blackhole attacks. Journal of Cybersecurity and Privacy, 2(1), 124-153.

[15] Khan, A. B. F., Lalitha, H. R., Devi, S. K., & Rajalakshmi, C. N. (2022). A multi-attribute based trusted routing for embedded devices in MANET-IoT. Microprocessors and Microsystems, 89, 104446. https://doi.org/10.1016/j.micpro.2022.104446

[16] Ali, A. A., Hussain, M. M., & Rao, A. S. (2024). Enhancing security in the Internet of Things: A trust-based protocol for resilient communication. SN Computer Science, 5, 4. https://doi.org/10.1007/s42979-023-02329-4

[17] Khan, A. B. F., Hussain, M. M., Devi, S. K., & Gunavathie, M. A. (2023). DDoS attack modeling and resistance using trust-based protocol for the security

of Internet of Things. Journal of Engineering Research, 11(2), 100058. https://doi.org/10.1016/j.jer.2023.100058

[18] Mansour M., Gamal A., Ahmed A., said L., Herencsar A. E. N., and Soltan A., Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions, Energies. (2023) 16, no. 8, https://doi.org/10.3390/en16083465, 3465.

[19] Park H., Song S., Nguyen T., and Park L., Machine Learning for Internet of Things: Applications and Discussion, 2024 International Conference on Artificial Intelligence in Information and Communication, 2024.

[20] Shanmugapriya R. and Svn S. K., An Energy Efficient Swan Intelligent Based Clustering Technique (SICT) With Fuzzy Based Secure Routing Protocol in IoT, Peer-to-Peer Networking and Applications. (2024) 17, no. 4, 1830–1864, https://doi.org/10.1007/s12083-024-01670-6.

[21] Albinali H. and Azzedin F., Towards RPL Attacks and Mitigation Taxonomy: Systematic Literature Review Approach, IEEE Transactions on Network and Service Management. (2024) 21, no. 5, 5215–5238, https://doi.org/10.1109/TNSM.2024.3386468.

[22] Burange A. W. and Deshmukh V. M., Trust Based Secured Routing System for Low Powered Networks, Journal of Integrated Science & Technology. (2023) 11.

[23] Krari A., Hajami A., and Jarmouni E., Detecting the RPL Version Number Attack in IoT Networks Using Deep Learning Models, International Journal of Advanced Computer Science and Applications. (2023) 14, no. 10, https://doi.org/10.14569/IJACSA.2023.0141065.