Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

An Adaptive Fuzzy Trust-Based Framework for Secure RPL Routing in IoT Networks

Mukul Shukla[1], Lalji Prasad[2]
[1]*Ph.D. Scholar, Department of Computer Science & Engineering, SAGE University, Indore, INDIA*
[2]*Professor, Department of Computer Science & Engineering, SAGE University, Indore, INDIA*
mukul@sgsits.ac.in, hoi.iac@sageuniversity.in

ARTICLE INFO

Received: 03 Nov 2024

Revised: 20 Nov 2024

Accepted: 29 Dec 2024

ABSTRACT

Internet of Things (IoT) networks based on the Routing Protocol for Low-Power and Lossy Networks (RPL) are highly susceptible to malicious node attacks, which can significantly degrade network performance and reliability. This paper proposes an Adaptive Fuzzy Trust–Based RPL mechanism that dynamically evaluates node behavior using a multi-dimensional fuzzified trust assessment model incorporating packet forwarding ratio, energy consumption patterns, control message behavior, and cooperative trust feedback. By leveraging fuzzy logic, the proposed approach effectively handles uncertainty and imprecision in trust evaluation under dynamic network conditions. An adaptive fuzzy thresholding mechanism analyzes global fuzzy trust distributions to accurately detect and classify malicious nodes. Extensive simulations conducted in the Cooja simulator on Contiki OS demonstrate substantial improvements in Packet Delivery Ratio, End-to-End delay, Throughput, and Power Efficiency compared to existing trust-based RPL schemes. Results show significant gains in Packet Delivery Ratio (PDR), End-to-End Delay, Throughput, and Power Efficiency compared to existing RPL-based trust models. Specifically, the fuzzy trust framework achieves up to 25% improvement in PDR, 18% reduction in End-to-End Delay, 20% improvement in Throughput, and 15% improvement in Power Efficiency.

Keywords: Fuzzy Trust-Based Routing, IoT Security, RPL Protocol, Malicious Node

INTRODUCTION

The Internet of Things (IoT) is transforming various industries, including smart cities, healthcare, and industrial automation. However, IoT networks face significant security challenges due to their low-power nature and susceptibility to malicious node attacks [1]. The Routing Protocol for Low-Power and Lossy Networks (RPL), a widely used IoT routing standard, is vulnerable to packet dropping, excessive control message injection, and energy depletion attacks, leading to decreased Packet Delivery Ratio (PDR), increased end-to-end (E2E) delay, poor throughput, and high energy consumption [2].

To mitigate these threats, we propose an Adaptive Fuzzy Trust–Based RPL protocol that dynamically detects and isolates malicious nodes using a multi-dimensional fuzzified trust assessment model [3]. The proposed model evaluates Behavioral Trust, Energy Trust, Control Message Trust, and Cooperative Trust, which are converted into linguistic variables and processed through a fuzzy inference system to accurately assess node trustworthiness under uncertain and dynamic network conditions [4]. A fuzzy-guided adaptive thresholding mechanism classifies nodes into trusted, suspicious, and malicious categories and effectively isolates malicious nodes from RPL routing operations. Simulation results demonstrate significant improvements compared to existing RPL protocol [5].

In addition, the proposed fuzzy trust management framework enhances network adaptability and robustness by continuously updating trust values based on real-time node behavior and historical interactions. By incorporating cooperative trust feedback and adaptive fuzzy rules, the framework minimizes false positives and false negatives in malicious node detection while maintaining low computational and communication overhead [6]. This lightweight yet intelligent trust management approach improves routing stability and strengthens IoT network resilience against insider and dynamic routing attacks, making it suitable for real-world and resource-constrained IoT applications [6]. Moreover, its scalable and decentralized design enables seamless deployment in large-scale IoT networks without relying on centralized control or extensive parameter tuning.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

RELATED WORK

Azzedin, F., et al. (2023), In IoT environments where devices have limited energy and resources, attacks that drain battery power can be very dangerous. Flooding attacks and version number manipulation attacks are major security issues in the RPL routing protocol. One study introduces a trust-based technique to protect RPL networks from these attacks. The results show that version number attacks spread quickly and cause serious damage, while hello-message flooding attacks mostly affect the nearby area only. Their simulation proved that the trust-based method is effective in stopping both types of attacks and improving network resilience [1].

Alfriehat, N., et al. (2024), RPL plays an important role in IoT and sensor-based systems. However, if attackers target RPL, they can stop data from being delivered and waste network resources. Another research paper explains different RPL-related attacks, highlights their impact, and discusses possible protection strategies. It also compares earlier security studies to identify the most dangerous threats and give direction for future research. This work shows the importance of studying RPL-based attacks more deeply so that stronger security solutions can be developed [2].

Ioulianou, P. P., et al. (2019), Even though IoT devices are widely used today, they are still vulnerable to large-scale attacks such as Mirai and Chalubo botnet attacks. To protect RPL networks from denial-of-service (DoS) attacks, one study presents an Intrusion Detection System (IDS). The IDS uses a threshold-based method and includes both centralized and distributed components. Experiments performed using ContikiOS and the Cooja simulator demonstrate that the IDS works well and produces very few false alarms, even in large IoT networks [3].

Paganraj, D., et al. (2024), In many cases, attackers focus on draining a node's memory and energy, which eventually causes the entire IoT system to stop working. Most traditional RPL security techniques waste energy and reduce device lifetime. A new protocol called DE2RA-RPL introduces a lightweight and efficient solution to defend against DAO flooding, rank manipulation, and version attacks. Simulation results prove that this method improves packet delivery, increases throughput, saves energy, and reduces delay when compared to the standard RPL protocol. This makes it suitable for critical communication systems, including emergency and automated applications [4].

Albinali, H., et al. (2024), RPL is widely used in low-power networks, but it still has several security weaknesses. A comprehensive survey of 175 research papers reviews different RPL attacks and defenses. It groups attacks into categories such as packet generation, packet dropping, and packet modification. It also discusses countermeasures like authentication, encryption, and isolating malicious nodes. The study recommends developing new and advanced techniques to protect RPL networks against routing-based attacks and stresses the need for efficient evaluation standards [5].

Adarbah et al. (2022), The IoT enables global connectivity for monitoring, processing, and analyzing device-generated data, but the large volume of data and open communication environment introduce significant security challenges. This paper reviews RPL security issues, particularly selective forwarding attacks, and introduces a secure ECDH-based authentication and key-agreement scheme. The proposed method ensures strong mutual authentication, secure session key distribution, and resistance to known attacks, while maintaining low computational and communication overhead—making it practical for resource-constrained IoT environments [6].

Alsukayti, I. S., et al. (2023), The internal structure of RPL makes it especially vulnerable to routing attacks during network topology formation. Experimental research shows that these attacks greatly affect quality of service (QoS), network stability, and energy efficiency, especially when networks become large or attackers are sophisticated. In extreme scenarios, the RPL network performance can drop by more than 90%, and energy and resource usage may increase by up to 200% [7].

Mosa, H., et al. (2024), IoT networks are used everywhere, and this widespread use makes them attractive targets for cyber-attackers. Machine learning techniques are increasingly being used to detect and prevent RPL-specific attacks such as Hello flooding, rank attacks, blackhole attacks, and version number attacks. One study tested Random Forest and KNN classifiers on more than 160 million data records. The Random Forest model achieved 99% accuracy, while KNN reached 98% accuracy in identifying malicious network behavior. This proves that machine learning algorithms can effectively detect IoT routing attacks and support reliable security monitoring [8]. However, the high computational and data requirements of such models motivate the exploration of lightweight alternatives, such as fuzzy trust–based mechanisms, for resource-constrained IoT environments.

Gonen, S., et al. (2024), The Internet of Things also includes the Internet of Medical Things (IoMT), where medical devices share sensitive health data. While IoMT brings huge benefits, it also creates cybersecurity challenges. To protect these systems, encryption and strong authentication are essential. In one study, researchers analyzed flood-based attacks under single-attacker and multiple-attacker cases. They used artificial intelligence and forensic techniques to detect threats in real time. Their AI model achieved 99.9% accuracy, showing its very high reliability for security monitoring in IoT systems. This demonstrates the importance of AI in strengthening IoT networks [9].

Wakili et al. (2024), address the performance and security challenges faced by RPL in IoT systems. They present an AI-powered solution called NANTAR, designed to improve both routing efficiency and security. Compared to standard RPL, NANTAR increases network throughput by 20%, reduces delay by 20-30%, and lowers false detection rates by 15-20%. It also performs well in large-scale IoT deployments while maintaining low energy usage, making it a reliable method for strengthening IoT routing security [10].

Rajasekar, V. R., et al. (2024), Several types of isolation attacks target the RPL protocol, such as Blackhole Attacks, Selective Forwarding Attacks, and Destination Advertisement Object Inconsistency Attacks (DAO-IA). These attacks interrupt normal data transmission in IoT networks, causing nodes to be cut off from the network. One study examined different techniques used to defend against such attacks and found that most research focuses on reducing power consumption. However, performance factors like delay and control-packet overhead are less studied [11].

Rouissat, M., et al. (2023), As IoT devices grow in number, their limited processing power and battery life make them vulnerable to cyber-attacks, especially flooding attacks. Since standard RPL lacks built-in security features, attackers can easily exploit it. A malicious node can send a large amount of fake control information, known as a DIO Flooding (DIOF) attack, which overwhelms the network. Results show that such attacks cause network control traffic to increase by 500%, power consumption by 210%, packet delivery ratio (PDR) drops by 32%, and delay increases by 192%. To solve this, researchers propose DIOF-Secure RPL (DSRPL), a lightweight method that can identify and control the attack in a few seconds. Their solution reduced energy use and network overhead by 80% [12].

Alamiedy, T. A., et al. (2021), RPL is widely used in IoT, but it struggles with energy efficiency and is exposed to Distributed Denial of Service (DDoS) attacks. To address this, another study introduced an ensemble feature-selection technique to detect DDoS attacks in RPL networks. It uses three bio-inspired optimization algorithms to pick the best features for attack detection, and then applies Support Vector Machine (SVM) for classification. This method improves DDoS detection accuracy and makes IoT routing more secure. However, the approach introduces additional computational overhead and relies on centralized learning, which may limit its applicability in highly resource-constrained IoT environments [13].

Bang, A. O., et al. (2022), Routing-based attacks make protecting RPL networks a difficult task. A comprehensive review studied different RPL security threats and defense solutions. It created a new classification system for RPL attacks based on control-message manipulation and mapped each attack type to possible defense techniques. The review also compared tools, methods, and evaluation techniques used in previous studies. It highlights remaining research challenges and encourages further security improvements for RPL networks [14].

Kannan, A., et al. (2024), IoT networks also require intelligent security solutions, as traditional rule-based intrusion systems cannot fully protect them. To address this, one study introduced an Intelligent Intrusion Detection System (IDS) called NGCA (Neuro-Genetic Classification Algorithm), which combines neural networks with genetic algorithms for optimal attack detection. When tested on the NSL-KDD dataset, NGCA performed better than Decision Trees, Logistic Regression, and SVM models. It achieved high accuracy with low false alarms, proving its reliability for securing IoT networks [15].

Sridhar, K., et al. (2024), In addition, routing in IoT networks is difficult to secure due to device limitations such as low memory and battery power. RPL structures the network efficiently, but attackers can manipulate routing metrics through Routing Disruption Attacks (RDAs). To combat this, another research introduced RDAD, a method that uses Packet Delivery Ratio (PDR) analysis to find reliable routes and detect abnormal behavior. RDAD significantly improves packet delivery performance, reduces data loss, and achieved a 96.5% attack detection rate, making IoT routing safer [16]. However, its reliance on a single performance metric highlights the need for multi-dimensional and adaptive trust mechanisms, such as fuzzy-based trust evaluation, to handle complex and dynamic attack behaviors in IoT networks.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Wang, X., et al. (2024), Although RPL is useful for IoT networking, its design makes it vulnerable to sophisticated security attacks. Because of this, attackers can easily target and control network communication. One major challenge in improving RPL security is the shortage of high-quality datasets that specifically contain RPL-related attack scenarios. To address this, researchers developed a dedicated IoT dataset that includes common RPL attacks such as Blackhole, Hello Flooding, and Version Number attacks. After testing various machine learning models on this dataset, Random Forest gave the best results in detecting and reducing the impact of these attacks [17].

Ahmadi, K., et al. (2024), RPL is highly vulnerable to blackhole attacks, selective forwarding attacks, and rank manipulation attacks, which can severely disrupt network communication. Many IoT devices lack the processing power to run traditional cryptographic techniques. To overcome this limitation, researchers proposed a trust-based intrusion detection system using Recurrent Neural Networks (RNN). The system predicts routing behavior and detects unusual activity in real-time simulations. Results showed high accuracy and precision, enabling early detection and prevention of malicious nodes [18].

Gonen, S., et al. (2023), As IoT grows globally, cybersecurity becomes more critical because connected devices are often targeted by attackers. One study investigated the impact of flooding-based attacks on IoT systems by analyzing network traffic during attacks. The researchers used Texecom Cloud with packet mirroring to support real-time forensic analysis and avoid network overload. Artificial intelligence was used to identify attackers automatically, enabling continuous monitoring and improving the resilience of IoT systems [19].

OBJECTIVES

The primary objective of this article is to design and implement an Adaptive Fuzzy Trust–Based RPL routing protocol that effectively detects and mitigates malicious node behavior in low-power and lossy IoT networks. By integrating a multi-dimensional fuzzy trust assessment model, the proposed approach aims to accurately evaluate node trustworthiness using behavioral, energy, control message, and cooperative trust metrics under uncertain and dynamic network conditions. The objective is to overcome the limitations of traditional RPL security mechanisms by providing adaptive, lightweight, and intelligent trust-based routing decisions that enhance network security without imposing excessive computational or energy overhead on resource-constrained IoT devices.

Another key objective of this work is to evaluate the performance and effectiveness of the proposed fuzzy trust management framework through extensive simulations and comparative analysis. The study aims to demonstrate measurable improvements in critical network performance metrics, including Packet Delivery Ratio, End-to-End Delay, Throughput, and Power Efficiency, when compared with existing RPL and trust-based routing models. Furthermore, this article seeks to validate the robustness and scalability of the proposed solution in realistic IoT scenarios, ensuring its suitability for real-world, large-scale, and energy-constrained IoT applications while maintaining resilience against insider and dynamic routing attacks.

METHODS

Figure 1 presents the proposed Fuzzy Trust Management Architecture designed to secure RPL-based IoT networks by enabling adaptive and intelligent trust evaluation under uncertain and dynamic network conditions. The architecture is structured around three tightly coupled modules: Fuzzy Trust Score Calculation, Adaptive Fuzzy Trust Thresholding, and Malicious Node Detection and Mitigation. Together, these modules form a comprehensive trust management framework that continuously assesses node behavior, establishes trust classification, and identifies security threats in low-power and lossy network environments.

In the Figure 1, core of the architecture is the Fuzzy Trust Score Calculation module, which employs a multi-dimensional fuzzified trust assessment model. Behavioral Trust, Energy Trust, Control Message Trust, and Cooperative Trust metrics are transformed into linguistic variables (Low, Medium, High) and processed through a fuzzy inference system to capture uncertainty, imprecision, and dynamic variations in node behavior. The output of this module is a Global Fuzzy Trust Score, which provides a reliable and context-aware representation of node trustworthiness and serves as the foundation for subsequent trust decisions. By enabling smooth trust adaptation under fluctuating network conditions, this module significantly improves the accuracy and robustness.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

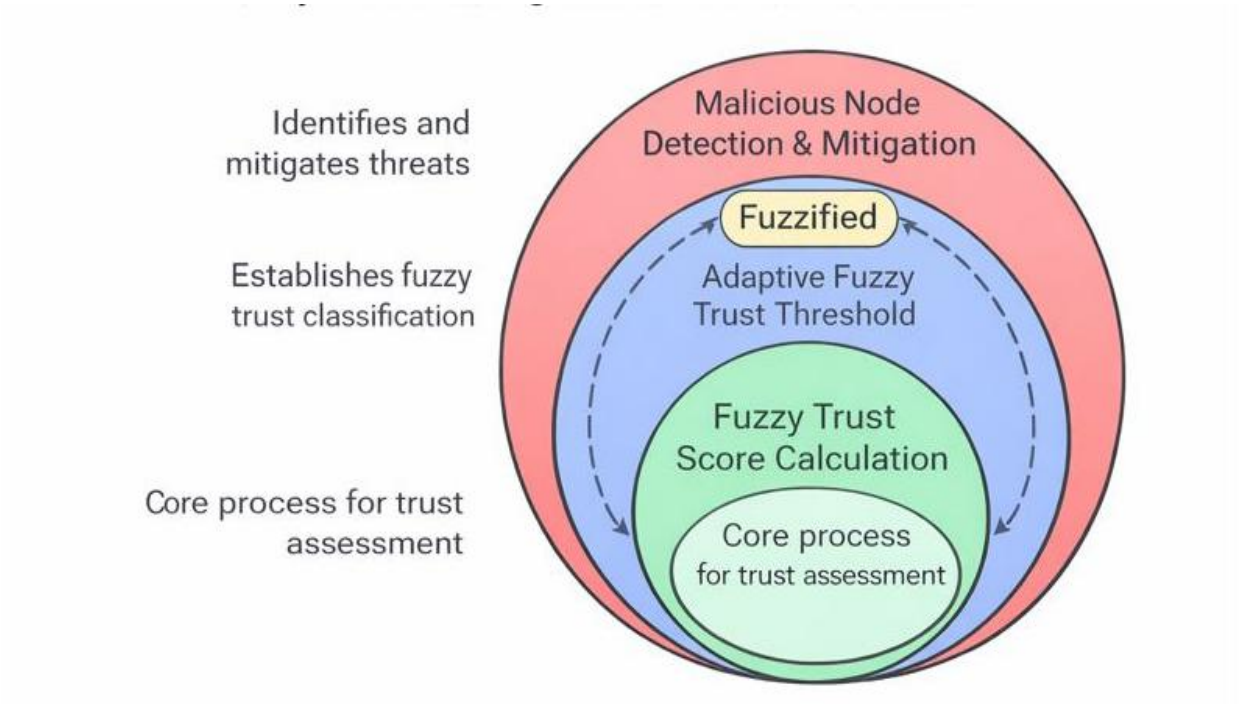

Figure 1. The architecture is the Fuzzy Trust Score Calculation module

Building upon the computed fuzzy trust scores, the Adaptive Fuzzy Trust Thresholding module dynamically determines an appropriate trust threshold based on the overall fuzzy trust distribution and current network conditions. This adaptive threshold enables accurate Malicious Node Detection, where nodes are classified as trusted, suspicious, or malicious. Nodes identified as malicious are isolated from RPL routing operations, including parent selection and control message propagation, thereby preventing routing disruption and energy depletion attacks. Through continuous fuzzy trust evaluation and adaptive mitigation, the proposed architecture enhances network resilience, routing stability, and energy efficiency, making it well suited for real-world and resource-constrained IoT deployments.

Furthermore, the integration of cooperative trust feedback and real-time monitoring in the fuzzy trust framework ensures that trust evaluations are continuously updated based on both historical and current node behavior. This enables the system to adapt to dynamic network changes, such as fluctuating traffic patterns or intermittent node failures, while minimizing false positives and false negatives in malicious node detection. By leveraging the inherent flexibility of fuzzy logic, the proposed mechanism can handle uncertainties and imprecise measurements in low-power and lossy networks, ensuring reliable routing decisions, reducing unnecessary energy consumption, and sustaining overall network performance even under adversarial conditions.

In addition, the proposed fuzzy trust–based architecture supports scalable and distributed trust management by allowing each node to locally compute and update trust values with minimal communication overhead. This decentralized operation aligns well with the constrained nature of IoT environments, as it avoids reliance on centralized authorities and reduces control message overhead. As a result, the framework maintains efficient routing performance while preserving node autonomy and network scalability in large-scale IoT deployments. The lightweight fuzzy inference process ensures low computational complexity, making it suitable for resource-limited sensor nodes. Moreover, localized trust computation enhances fault tolerance and enables faster response to malicious activities without introducing significant latency or energy overhead. Moreover, the adaptive nature of the fuzzy trust mechanism enables long-term network sustainability by continuously learning from evolving attack patterns and normal behavioral changes. This continuous adaptation strengthens overall network robustness and ensures consistent security enforcement throughout the operational lifetime of the IoT system.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

Algorithm 1 continuously evaluates each RPL node using four trust metrics in [0,1]. It computes Behavioral Trust as forwarded/received packets, Energy Trust as residual/initial energy, Control Message Trust as one minus excess control messages over a maximum, and Cooperative Trust as the average neighbor feedback. These values are normalized, fuzzified into Low/Medium/High, processed through fuzzy IF–THEN rules, aggregated, and defuzzified via the centroid method to output an updated Global Trust Score (GTS_i) for routing and attacker isolation.

In addition, the algorithm operates in a periodic and event-driven manner, allowing trust values to adapt dynamically to network conditions such as mobility, congestion, and energy depletion. At each evaluation interval, historical trust values are combined with the newly computed GTSi using a weighted update factor to smooth abrupt fluctuations and prevent transient errors from unfairly penalizing nodes. Nodes whose GTSii falls below a predefined adaptive threshold are gradually isolated by reducing their routing preference and limiting their participation in DIO/DAO dissemination, rather than being immediately removed, which minimizes false positives. This continuous learning and gradual mitigation strategy ensures stable RPL topology formation, improves resilience against insider attacks, and maintains energy-efficient routing while preserving overall network connectivity. Consequently, the network can respond intelligently to evolving attack patterns while maintaining reliable data delivery and low control overhead in highly dynamic IoT environments. Moreover, this adaptive and incremental isolation process supports long-term network stability by balancing security enforcement with routing flexibility and fairness.

Algorithm 1: Fuzzy Logic–Based Trust Score Calculation

Input:
Packet forwarding statistics, residual energy, control message count, neighbor trust feedback

Output:
Global Trust Score (GTS_i) for node n_i

Step 1: Initialize trust parameters
$BT_i, ET_i, CMT_i, CT_i \in [0, 1]$

Step 2: Monitor node n_i continuously during RPL operation.

Step 3: Compute Behavioral Trust (BT_i)
$BT_i \leftarrow P_i\_forwarded / P_i\_received$

Step 4: Compute Energy Trust (ET_i)
$ET_i \leftarrow E_i\_residual / E_i\_initial$

Step 5: Compute Control Message Trust (CMT_i)
$CMT_i \leftarrow 1 - (C_i\_excess / C\_max)$

Step 6: Compute Cooperative Trust (CT_i)
$CT_i \leftarrow (1 / N_i) \times \Sigma_{j=1}^{N_i} T_{j \rightarrow i}$

Step 7: Normalize $\{BT_i, ET_i, CMT_i, CT_i\}$ to the range [0, 1].

Step 8: Fuzzify the normalized trust values into linguistic variables {Low, Medium, High}.

Step 9: Apply fuzzy IF–THEN inference rules to evaluate node trust.

Step 10: Aggregate fuzzy rule outputs.

Step 11: Defuzzify the aggregated output using the centroid method.

Step 12: Output the resulting Global Trust Score *GTSi* for node *ni*, representing its overall trustworthiness derived from fuzzy inference and multi-dimensional trust evaluation.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

The Algorithm 2 dynamically determines a trust threshold for RPL networks using fuzzy logic. It collects and normalizes all nodes' Global Trust Scores, analyzes network conditions, and fuzzifies trust levels into linguistic terms. Fuzzy inference rules evaluate overall network trust, which is aggregated and defuzzified to produce an adaptive threshold for secure routing and malicious node detection.

Furthermore, the adaptive threshold computation is periodically refined to reflect temporal variations in node behavior, traffic load, and topology changes inherent to RPL-based IoT networks. By incorporating statistical dispersion of Global Trust Scores—such as mean and variance—the algorithm prevents overly strict or lenient threshold selection in heterogeneous environments. The resulting threshold is broadcast to all nodes and used consistently during parent selection and route maintenance, ensuring network-wide coherence in trust decisions. This adaptive mechanism reduces false positives in malicious node detection, enhances robustness against coordinated attacks, and maintains a balance between security enforcement and routing stability.

Algorithm 2: Adaptive Fuzzy Trust Threshold Calculation

Input:
Global Trust Scores (GTS) of all nodes, fuzzy trust distribution, current network conditions

Output:
Adaptive Trust Threshold

Step 1: Collect the Global Trust Scores (GTS) of all participating nodes in the RPL network.

Step 2: Monitor and analyze current network conditions, including node density, traffic load, and variations in trust behavior.

Step 3: Normalize the collected Global Trust Scores to ensure all values lie within the range [0,1].

Step 4: Fuzzify the normalized trust scores into linguistic variables such as *Low*, *Medium*, and *High* using predefined membership functions.

Step 5: Apply fuzzy IF–THEN inference rules to evaluate the overall network trust condition based on the fuzzified trust inputs.

Step 6: Aggregate the outputs of all activated fuzzy rules to obtain a combined fuzzy threshold representation.

Step 7: Defuzzify the aggregated fuzzy threshold using the centroid method to compute a crisp threshold value.

Step 8: Adaptively update the trust threshold by incorporating historical trust trends along with current fuzzy inference results.

Step 9: Output the final Adaptive Trust Threshold $T\_adaptive$ for malicious node classification and trust-based routing decisions.

The Algorithm 3 detects and mitigates malicious nodes using trust scores and an adaptive threshold. For each node, it compares GTS_i with T_adaptive and a minimum margin T_min. Nodes with $GTS_i \geq$ T_adaptive are trusted; those with T_adaptive > $GTS_i \geq$ T_min is marked suspicious and monitored. If $GTS_i <$ T_min, the node is classified malicious and isolated by removing it from parent selection, forwarding paths, and control message exchange. Additionally, the mitigation process follows a graded response strategy to balance security and network performance. Instead of immediate and permanent exclusion, isolated nodes may undergo a probation phase during which their behavior is closely observed under restricted participation. This adaptive and progressive mitigation approach preserves overall routing stability in dynamic RPL-based IoT networks.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

Algorithm 3: Malicious Node Detection and Trust-Based Mitigation

Input:
Global Trust Scores (GTS) of all nodes, Adaptive Trust Threshold $T\_adaptive$

Output:
Detection, classification, and isolation of malicious nodes

Step 1: Collect the Global Trust Score $GTSi$ of each node niobtained from the fuzzy trust evaluation process.

Step 2: Retrieve the Adaptive Trust Threshold $T\_adaptive$ computed using the adaptive fuzzy trust thresholding mechanism.

Step 3: Compare the Global Trust Score of each node with the Adaptive Trust Threshold to assess its trustworthiness.

Step 4: Classify a node as trusted if $GTSi \geq Tadaptive$, allowing it to participate fully in RPL routing and parent selection.

Step 5: Classify a node as suspicious if $Tadaptive > GTSi \geq Tmin$ where $Tmin$ represents a predefined minimum trust margin; such nodes are closely monitored for behavioral changes.

Step 6: Classify a node as malicious if $GTSi < Tmin$ indicating persistent abnormal or harmful behavior.

Step 7: Isolate malicious nodes by excluding them from RPL parent selection, data forwarding paths, and control message propagation.

Step 8: Update routing tables and trust records of neighboring nodes to prevent future interactions with isolated malicious nodes.

Step 9: Continuously re-evaluate node trust scores to allow recovery of falsely isolated nodes and ensure adaptability to dynamic network conditions.

Fuzzy Trust Assessment and Adaptation Model

To address uncertainty, dynamic behavior, and imprecise observations in IoT environments, we introduce a multi-dimensional Fuzzy Trust Adaptation Model for secure RPL-based routing. The proposed model evaluates node trustworthiness using multiple trust components that collectively capture routing behavior, energy usage patterns, control message activity, and cooperative feedback. Instead of relying solely on crisp values, each trust metric is fuzzified and processed through a fuzzy inference mechanism to improve robustness and accuracy in malicious node detection.

The fuzzy inference system applies a set of well-defined IF–THEN rules to combine the fuzzified trust inputs and derive a comprehensive trust evaluation that reflects both individual node behavior and overall network conditions. By leveraging linguistic variables and membership functions, the model effectively handles noise, incomplete information, and transient fluctuations commonly observed in low-power and lossy networks. The resulting defuzzified trust score is continuously updated and integrated into RPL routing decisions, enabling adaptive parent selection and timely mitigation of malicious or energy-draining nodes while maintaining routing stability and energy efficiency. Furthermore, the adaptive nature of the fuzzy trust model allows it to respond promptly to evolving attack patterns and changing traffic dynamics without requiring manual reconfiguration. This flexibility makes the proposed approach robust and scalable, ensuring consistent security and performance even as network size, topology, and threat intensity change over time.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Trust Components

- **Behavioral Trust (BT):**

  Measures historical routing behavior using the Packet Forwarding Ratio (PFR) to detect packet dropping and selective forwarding attacks. The observed PFR values are fuzzified into linguistic levels (Low, Medium, High) to accommodate fluctuations in traffic conditions.

- **Energy Trust (ET):**

  Evaluates residual energy patterns to detect abnormal power consumption indicative of energy depletion or denial-of-service attacks. Energy values are mapped to fuzzy sets to tolerate normal energy variations in resource-constrained IoT nodes. This fuzzy energy trust assessment enables early detection of energy-based attacks while preventing false alarms caused by legitimate workload fluctuations, thereby extending overall network lifetime.

- **Control Message Trust (CMT):**

  Monitors the frequency of RPL control messages (DIS/DIO/DAO) to identify excessive or abnormal control traffic. Fuzzification enables the detection of subtle control flooding behavior that may not be captured by fixed thresholds. By correlating control message patterns with other trust metrics, the mechanism accurately distinguishes malicious signaling activity from legitimate topology maintenance operations.

- **Cooperative Trust (CT):**

  Aggregates trust recommendations from neighboring nodes to validate local trust assessments and enhance reputation accuracy. Neighbor feedback is incorporated as fuzzy inputs to reduce the impact of isolated false observations. This collaborative trust evaluation strengthens resilience against insider and on–off attacks, where malicious nodes attempt to alternate between normal and abnormal behavior.

Fuzzy Trust Score Computation

Each node computes a Global Fuzzy Trust Score (FTS) using a weighted aggregation of the fuzzified trust components:

$$FTS(i) = \alpha \cdot BT(i) + \beta \cdot ET(i) + \gamma \cdot CMT(i) + \delta \cdot CT(i)$$

where α, β, γ, δ are adaptive fuzzy weights that dynamically adjust according to network conditions and trust distribution.

Fuzzy Trust Levels and Interpretation

Based on the defuzzified trust score, nodes are classified into adaptive trust levels:

- **High Trust (FTS ≥ 0.85):**

  The node is highly reliable and fully eligible for RPL routing operations.

- **Moderate Trust (0.70 ≤ FTS < 0.85):**

  The node is stable but subjected to continuous fuzzy trust monitoring.

- **Low Trust (0.50 ≤ FTS < 0.70):**

  The node exhibits suspicious behavior and is restricted from critical routing roles.

- **Critical Trust (FTS < 0.50):**

  The node is considered malicious and is isolated from RPL routing activities.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Adaptive Fuzzy Trust Thresholding Mechanism

Instead of relying on static or fixed trust thresholds, the proposed security framework employs an Adaptive Fuzzy Trust Thresholding Mechanism that dynamically adjusts trust boundaries based on real-time network behavior and trust distribution. This mechanism continuously analyzes the global trust status of the network and incorporates uncertainty, variability, and dynamic node behavior through fuzzy logic. By avoiding rigid threshold values, the proposed approach enables more accurate and flexible identification of malicious nodes in highly dynamic and resource-constrained IoT environments.

The adaptive threshold TadaptiveT_{adaptive}Tadaptive is derived using a fuzzy statistical model based on the global trust score distribution, expressed as:

$$T\_\{adaptive\} = \mu(TS\_global) + k \times \sigma(TS\_global)$$

where TSglobal represents the average fuzzy trust score across the network, k is a sensitivity factor controlling anomaly detection aggressiveness, and μ and σ denote the mean and standard deviation of trust scores, respectively. These statistical parameters are further processed through fuzzy membership functions to generate a context-aware threshold that adapts to changing network conditions. As a result, the fuzzy thresholding mechanism reduces false positives and false negatives, enhances malicious node detection accuracy, and improves overall network stability and resilience.

Fuzzy Trust Threshold Interpretation

The proposed Fuzzy Trust Threshold Interpretation classifies network nodes based on their defuzzified trust scores and adaptive fuzzy thresholds, enabling accurate and flexible decision-making under uncertain network conditions. Instead of rigid binary classification, fuzzy trust levels allow gradual differentiation between trusted, suspicious, and malicious nodes, thereby improving detection accuracy and reducing false alarms.

- **Trusted State:**

  If the fuzzy trust score $TS \geq T\_adaptive$, the node is classified as trusted and safe. Such nodes are fully permitted to participate in RPL routing operations, including parent selection and control message forwarding.

- **Suspicious State:**

  If $T\_adaptive > TS \geq 0.50$, the node is classified as at risk. These nodes exhibit uncertain or fluctuating behavior and are subjected to continuous fuzzy trust monitoring and restricted routing roles until their trust level stabilizes.

- **Malicious State:**

  If $TS < 0.50$, the node is classified as malicious and is immediately isolated from the network. Fuzzy trust-based isolation prevents such nodes from participating in data forwarding and control message exchange, thereby mitigating routing and energy-based attacks.

Mitigation via Fuzzy Trust–Based Routing

The proposed security framework integrates Fuzzy Trust–Based Routing to effectively mitigate malicious node behavior in RPL-based IoT networks. Instead of relying solely on traditional RPL rank metrics, routing decisions are guided by defuzzified trust scores, enabling more reliable and attack-resilient parent selection under uncertain network conditions. By prioritizing nodes with higher fuzzy trust levels, the framework ensures stable routing paths, reduces packet loss, and prevents traffic redirection through compromised or unstable nodes. Additionally, the dynamic update of fuzzy trust scores allows routing decisions to adapt in real time to changes in node behavior and network conditions. This trust-aware routing strategy improves overall network resilience, maintains quality of service, and enhances energy efficiency in the presence of both insider and external attacks. As a result, the proposed approach supports scalable, secure, and sustainable routing operations suitable for long-term and large-scale IoT deployments.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Furthermore, the fuzzy trust–based routing mechanism incorporates a trust decay and recovery strategy, allowing trust values to dynamically adapt to changes in node behavior over time. Nodes exhibiting intermittent or improving behavior can gradually regain trust, while persistently malicious nodes experience rapid trust degradation and isolation. This adaptive mitigation approach not only minimizes false isolation but also enhances routing stability, energy efficiency, and overall network resilience, making the protocol well suited for dynamic and resource-constrained IoT environments.

- **Fuzzy Trust–Based Parent Selection:**

  Each node prioritizes neighboring nodes with high fuzzy trust levels during parent selection, rather than selecting parents solely based on RPL rank. By incorporating trust as a primary routing metric, the network avoids malicious or unstable nodes, thereby improving routing reliability and data delivery performance.

- **Fuzzy Trust Decay Mechanism:**

  A **fuzzy trust decay mechanism** is employed to gradually reduce a node's trust score when its behavior becomes inconsistent or fluctuates over time. This adaptive decay prevents abrupt trust drops due to transient network conditions while ensuring that persistently misbehaving nodes are progressively restricted from routing participation.

- **Distributed Fuzzy Attack Mitigation:**

  When a node's fuzzy trust score falls below the adaptive fuzzy threshold TadaptiveT_{adaptive}Tadaptive, neighboring nodes collaboratively initiate isolation actions. This distributed fuzzy mitigation approach ensures rapid and scalable attack handling without centralized control, effectively preventing the propagation of routing attacks and maintaining overall network stability.

RESULTS

Simulation Setups

In this study, we evaluate the performance of the proposed Fuzzy Trust–Based RPL security framework using a simulated IoT network consisting of 50 static sensor nodes. All simulations were conducted using the Cooja network simulator, a widely used and accurate Java-based simulation platform, operating within the Contiki OS environment designed for resource-constrained IoT devices. Cooja enables precise modeling of low-power wireless networks and supports detailed analysis of routing behavior, trust dynamics, and attack scenarios in RPL-based IoT networks.

The simulations were implemented using the Zolertia Z1 IoT platform, which is equipped with an MSP430 microcontroller unit (MCU) and a CC2420 IEEE 802.15.4-compliant transceiver. The platform operates within a voltage range of 1.8 V to 3.6 V, with a maximum clock frequency of 16 MHz, ensuring realistic energy consumption and communication behavior. The proposed fuzzy trust assessment, adaptive thresholding, and trust-based routing mechanisms were integrated into the RPL protocol stack within Contiki OS. This setup enabled comprehensive evaluation of fuzzy trust dynamics, malicious node mitigation effectiveness, and network performance metrics under realistic IoT operating conditions.

Network Configuration with Fuzzy Trust–Based RPL

The network configuration for evaluating the proposed Fuzzy Trust–Based RPL security mechanism is summarized in Table X. The simulation environment consists of 50 static IoT sensor nodes deployed over a 400 m² area, with a fixed transmission range of 10 m. This dense deployment enables effective evaluation of fuzzy trust interactions, cooperative trust aggregation, and malicious node influence within multi-hop RPL topologies.

Communication between nodes is established using the UDP transport protocol, while the IEEE 802.15.4 standard is employed for both the PHY and MAC layers, ensuring low-power and lossy network characteristics. Data packets are transmitted at regular intervals of 60 seconds, allowing the fuzzy trust system to continuously monitor node behavior, update trust values, and adapt routing decisions over time.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

To assess the robustness of the proposed fuzzy trust mechanism, five attacker nodes are introduced into the network to perform malicious activities such as packet dropping, excessive control message injection, and energy depletion attacks. The Unit Disk Graph Medium (UDGM) radio model is used to simulate realistic wireless communication. This configuration enables comprehensive evaluation of the fuzzy trust score calculation, adaptive fuzzy thresholding, and trust-based mitigation strategies under realistic IoT network conditions.

Table I: Network Configuration and Fuzzy Trust Parameters

Parameter	Value
Transmission Range	10 m
Number of Sensor Nodes	50
Deployment Area	400 m²
Transport Layer Protocol	UDP
PHY & MAC Layer Standard	IEEE 802.15.4
Data Packet Sending Interval	60 s
Number of Attacker Nodes	5
Radio Medium Model	Unit Disk Graph Medium (UDGM)
Trust Evaluation Interval	60 s
Trust Dimensions	BT, ET, CMT, CT
Fuzzy Input Variables	Low, Medium, High
Fuzzy Inference Method	Mamdani FIS
Defuzzification Technique	Centroid Method
Adaptive Fuzzy Threshold Type	Dynamic (Mean–Variance Based)
Trust Decay Factor	Adaptive (behavior-dependent)
Trust-Based Routing Metric	Fuzzy Trust Score (FTS)
Malicious Node Isolation Criterion	FTS < Adaptive Fuzzy Threshold

Performance Metrics

Average Power Consumption

Average power consumption represents the mean energy utilized by IoT nodes over a defined simulation period and is measured in milliwatts (mW). In the proposed fuzzy trust–based RPL framework, power efficiency is evaluated by monitoring node behaviour across active, idle, and sleep states. Additionally, nodes exhibiting abnormal or excessive energy usage patterns are assigned lower trust values, indicating potential malicious or misbehaving behaviour. By incorporating energy-aware fuzzy trust evaluation into routing decisions, the framework effectively reduces unnecessary energy expenditure while prolonging network lifetime and ensuring sustainable IoT operation. This adaptive energy-centric trust mechanism also helps balance load among nodes, preventing premature battery depletion of critical routing devices.

Throughput

Throughput denotes the rate at which data packets are successfully delivered from source nodes to destination nodes and is measured in kilobits per second (Kbps). By prioritizing high fuzzy trust nodes during routing and isolating low-trust or malicious nodes, the proposed approach ensures stable data forwarding paths, resulting in improved throughput even under adversarial network conditions. Furthermore, the adaptive fuzzy trust threshold dynamically adjusts routing preferences to mitigate congestion and packet loss caused by misbehaving nodes. This leads to more efficient bandwidth utilization and consistent data transmission performance across varying network loads.

End-to-End Delay

End-to-end delay refers to the total time taken by a data packet to traverse from the source to the destination and is measured in milliseconds (ms). This metric includes processing, transmission, propagation, and queuing delays. The adaptive fuzzy trust mechanism minimizes delay by preventing packet drops and reducing route recalculations caused by malicious behaviour, leading to faster and more reliable packet delivery. By prioritizing high-trust nodes in route selection, the framework ensures stable forwarding paths.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is defined as the ratio of the number of packets successfully received at the destination to the number of packets transmitted by the source, expressed as a percentage. In the proposed fuzzy trust–based RPL model, PDR is significantly enhanced due to accurate malicious node detection, adaptive trust thresholding, and trust-based routing decisions that ensure only reliable nodes participate in data forwarding.

6. DISCUSSION

Experimental Setup and Attack Scenario

Figure 2 illustrates the simulated IoT network topology used to evaluate the proposed Adaptive Fuzzy Trust–Based RPL security mechanism. The network consists of multiple static sensor nodes deployed within a defined communication range, with Node 1 configured as the sink node responsible for collecting data from all participating nodes. The green shaded region represents the wireless communication coverage area, while blue directional arrows indicate active data transmission paths established by the RPL routing protocol. Under normal operation, data packets are forwarded through multi-hop routes toward the sink node based on routing metrics and trust-aware parent selection.

Figure 2. The simulated IoT network topology

To rigorously assess the effectiveness of the fuzzy trust mechanism, the network is subjected to multiple coordinated routing attacks that exploit RPL vulnerabilities. A Flooding Attack is launched by Nodes 51 and 52, which generate excessive control and data packets to congest the network, increase energy consumption, and degrade throughput. A Version Number Attack is performed by Nodes 53 and 54, where manipulated routing updates are disseminated to mislead neighbouring nodes and trigger unnecessary topology reconstructions. Additionally, a Sinkhole Attack is initiated by Node 55, which falsely advertises optimal routing metrics to attract network traffic, thereby disrupting legitimate data forwarding and enabling selective packet dropping.

The proposed fuzzy trust management framework continuously monitors node behaviour during these attack scenarios by evaluating behavioural, energy, control message, and cooperative trust parameters. These trust values are fuzzified and processed through a fuzzy inference system to dynamically assess node trustworthiness under uncertain and adversarial conditions. Red-circled nodes in Figure 2 highlight the malicious and suspicious nodes identified by the fuzzy trust mechanism. Once a node's defuzzified trust score falls below the adaptive fuzzy threshold, it is isolated from routing operations through fuzzy trust–based mitigation and parent re-selection, ensuring secure and stable data delivery. This experimental setup enables comprehensive evaluation of attack detection accuracy, routing resilience, and performance improvements achieved through adaptive fuzzy trust–based RPL security.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Packet Delivery Ratio (PDR)

Figure 3 presents a comparative analysis of the Packet Delivery Ratio (PDR) under three network conditions: RPL with Attack, Existing Trust-Based RPL with Attack, and the Proposed Adaptive Fuzzy Trust–Based RPL with Attack. The results demonstrate that the proposed fuzzy trust–based RPL scheme consistently achieves the highest PDR across all evaluated categories. This improvement is attributed to the fuzzy trust evaluation mechanism, which accurately identifies malicious and unstable nodes by processing multiple trust dimensions under uncertain network conditions and dynamically isolates them from routing operations.

In contrast, the existing trust-based RPL approach exhibits moderate PDR performance, as it relies on rigid trust thresholds and limited adaptability to fluctuating node behaviour, leading to delayed or imprecise malicious node detection. The standard RPL with attack scenario performs the worst due to its lack of trust awareness, resulting in frequent packet drops, route disruptions, and malicious traffic forwarding. Overall, the superior PDR achieved by the proposed method highlights the effectiveness of fuzzy inference–driven trust assessment and adaptive fuzzy thresholding, which enable resilient routing decisions and significantly enhance data delivery reliability in adversarial IoT environments.

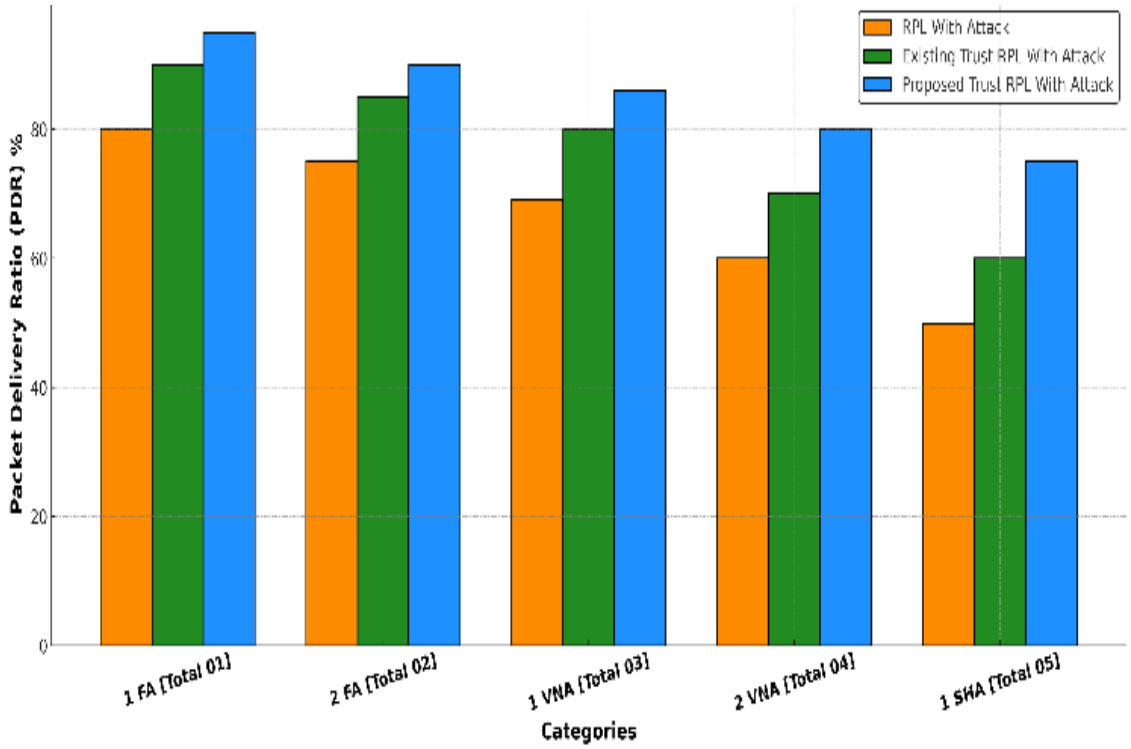

Figure 3. Compare Packet Delivery Ratio (PDR)

End-to-End Delay

Figure 4 illustrates the comparative End-to-End Delay (in milliseconds) for three network scenarios: RPL with Attack, Existing Trust-Based RPL with Attack, and the Proposed Adaptive Fuzzy Trust–Based RPL with Attack. The results show that the proposed fuzzy trust–based RPL consistently achieves the lowest end-to-end delay among all schemes. This improvement is primarily due to the fuzzy trust mechanism, which continuously evaluates node behaviour using behavioural, energy, control message, and cooperative trust parameters. Malicious and unstable nodes are identified and isolated through adaptive fuzzy thresholding, preventing them from participating in routing paths and reducing retransmissions and route recalculations. Additionally, prioritizing high-trust nodes during parent selection ensures stable multi-hop routes, thereby minimizing congestion and latency variations under adversarial conditions.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

In contrast, the existing trust-based RPL exhibits a moderate delay reduction because it relies on static trust thresholds and lacks the flexibility to adapt to dynamic node behaviour, resulting in occasional routing through suspicious nodes. The standard RPL under attack experiences the highest delay due to frequent packet drops, misrouting, and congestion caused by malicious nodes. Overall, the results demonstrate that the fuzzy inference–driven trust assessment and adaptive fuzzy routing decisions of the proposed framework significantly enhance network responsiveness, improve routing stability, and reduce latency in IoT networks under adversarial conditions.

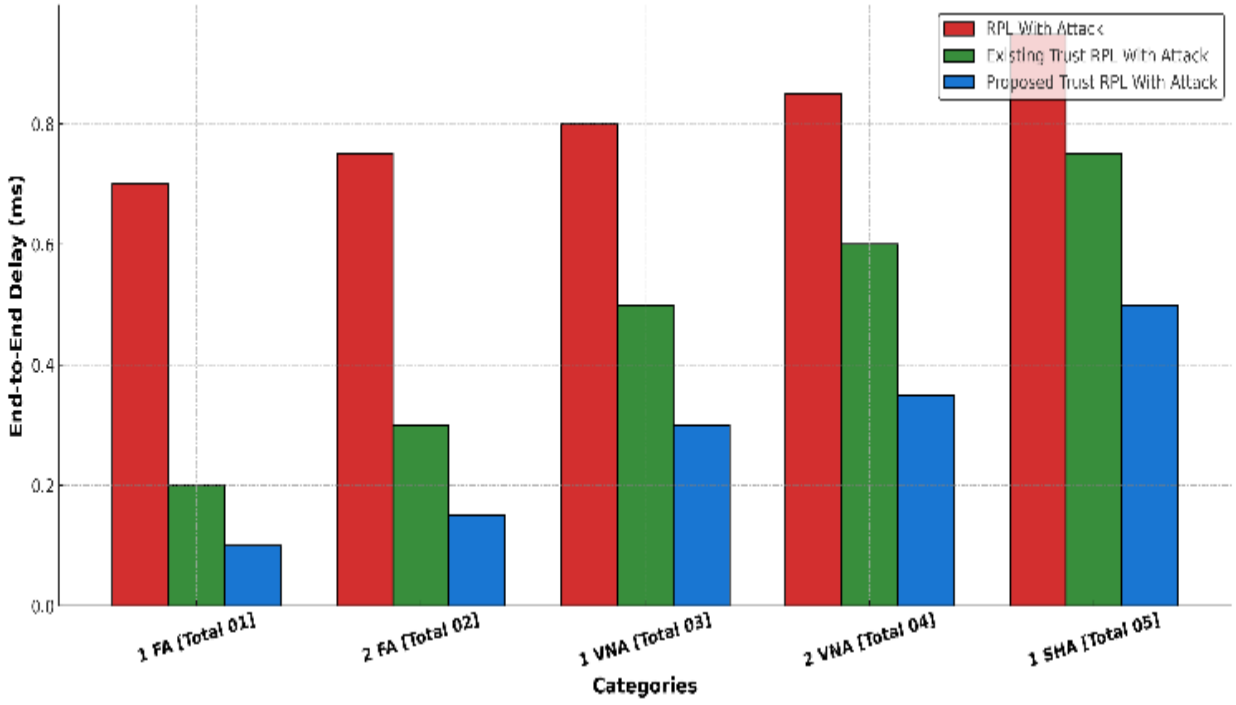

Figure 4. Compare End-to-End Delay (ms)

Throughput

Figure 5 compares the network throughput (in Kbps) across three scenarios: RPL with Attack, Existing Trust-Based RPL with Attack, and the Proposed Adaptive Fuzzy Trust–Based RPL with Attack. The results clearly demonstrate that the proposed fuzzy trust–based RPL consistently achieves the highest throughput among all evaluated schemes. This improvement is attributed to the fuzzy trust evaluation mechanism, which continuously monitors node behaviour across multiple dimensions—including behavioural, energy, control message, and cooperative trust—and dynamically isolates malicious or unstable nodes from the routing process. By ensuring that data packets are forwarded only through high-trust nodes, the proposed framework reduces packet loss, avoids network congestion, and maintains stable multi-hop routes, resulting in significantly higher data delivery rates.

In contrast, the existing trust-based RPL shows moderate throughput improvement because it relies on static trust thresholds and limited adaptability to dynamic node behaviour, causing occasional routing through suspicious nodes and resulting in packet drops. The standard RPL under attack performs the worst, as malicious nodes disrupt routing paths, drop packets, and introduce retransmissions, leading to severe degradation in throughput. Overall, the results demonstrate that adaptive fuzzy trust-based routing not only mitigates the impact of insider and external attacks but also maintains reliable data flow and network efficiency, highlighting the robustness and effectiveness of the proposed framework for IoT networks under adversarial conditions. Moreover, the continuous trust updates and adaptive parent selection reduce route instability and frequent reconfigurations, further contributing to sustained throughput performance. These findings confirm that the proposed approach achieves a favorable balance between security enforcement and communication efficiency in dynamic IoT environments.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

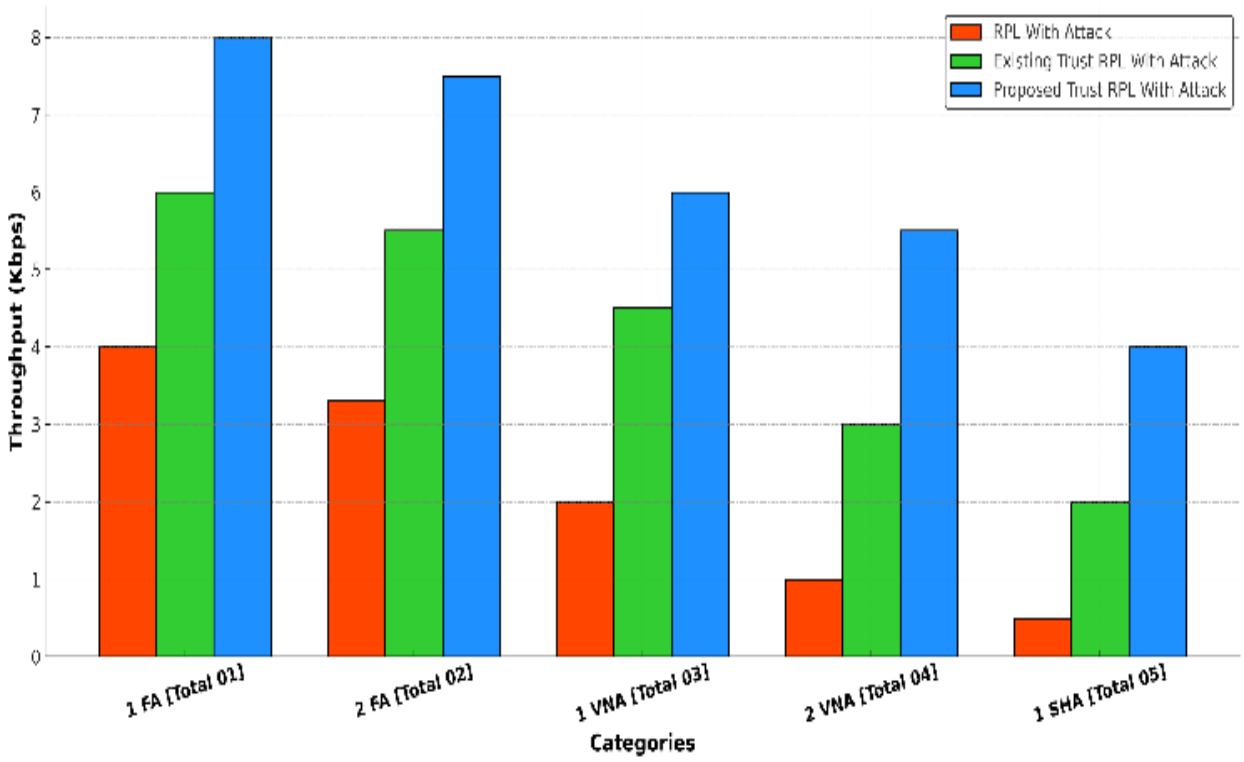

Figure 5. Compare Throughput (Kbps)

Power Consumption

Figure 6 illustrates the comparative power consumption (in milliwatts) for three network scenarios: RPL with Attack, Existing Trust-Based RPL with Attack, and the Proposed Adaptive Fuzzy Trust–Based RPL with Attack. The results demonstrate that the proposed fuzzy trust–based RPL consumes the least power among all schemes. This improvement is primarily due to the fuzzy trust mechanism, which continuously evaluates node behaviour across multiple trust dimensions—behavioural, energy, control message, and cooperative trust—and dynamically isolates malicious or unstable nodes from routing operations. By preventing compromised nodes from participating in packet forwarding, the framework reduces unnecessary retransmissions, excessive control message propagation, and energy wastage, thereby improving overall network energy efficiency.

In contrast, the existing trust-based RPL exhibits moderate energy savings, as static trust thresholds provide limited adaptability to dynamic node behaviour, causing occasional routing through nodes with fluctuating or suspicious activity. The standard RPL under attack consumes the highest power, as malicious nodes introduce congestion, repeated retransmissions, and unnecessary control traffic, leading to inefficient energy utilization. Overall, these results highlight that the adaptive fuzzy trust–based routing and thresholding mechanisms not only enhance security and reliability but also optimize energy consumption, making the proposed approach highly suitable for resource-constrained IoT networks.

Moreover, the observed reduction in power consumption directly contributes to prolonged network lifetime and improved sustainability of IoT deployments, particularly in battery-operated and unattended environments. By intelligently balancing security enforcement with energy-aware routing decisions, the proposed adaptive fuzzy trust–based RPL avoids excessive isolation of benign nodes while ensuring efficient utilization of network resources. This energy-efficient behaviour is critical for large-scale and long-term IoT applications, where minimizing maintenance costs and extending node operational lifetime are key performance objectives. Additionally, the adaptive fuzzy trust mechanism enables the network to dynamically respond to energy fluctuations and attack-induced overhead, ensuring consistent performance without compromising security or scalability.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

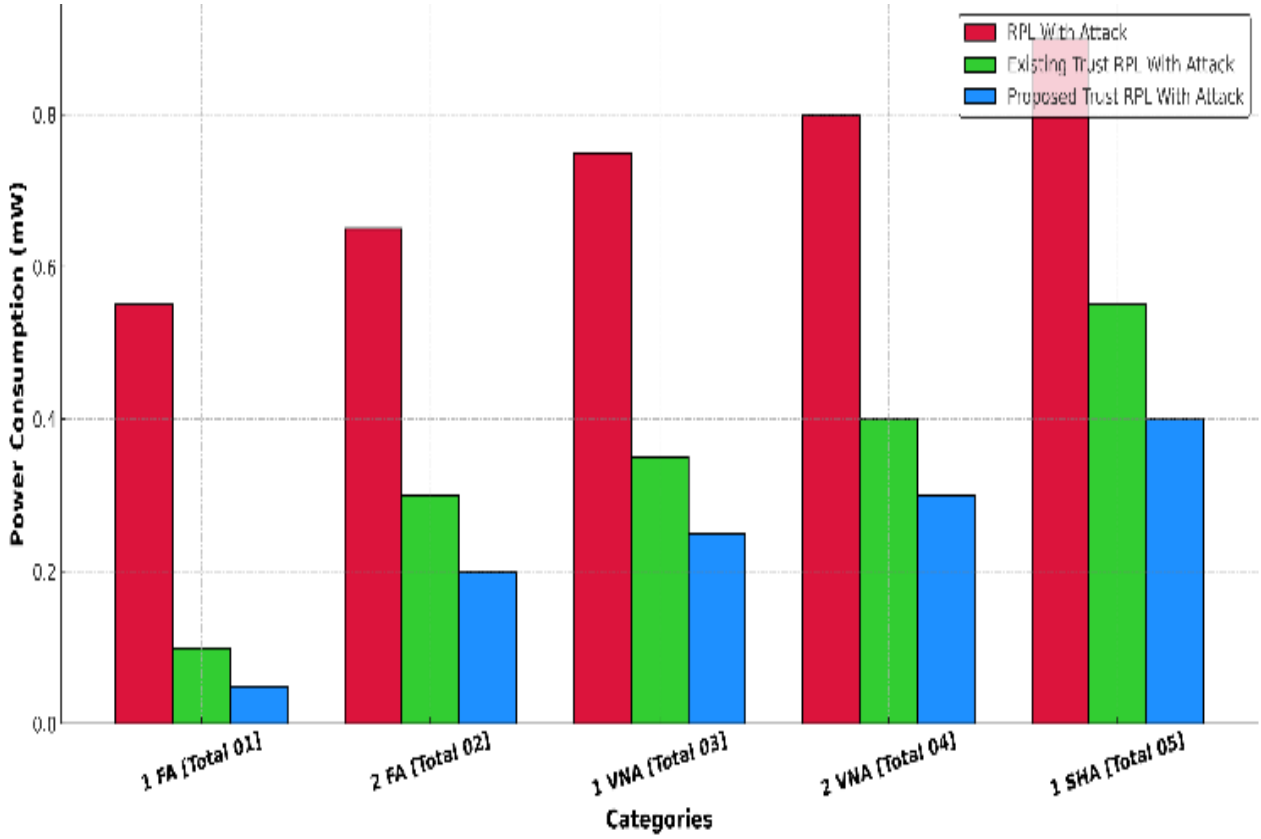

Figure 6. Compare Power Consumption (mW)

CONCLUSION

This research presented an Adaptive Fuzzy Trust–Based RPL security framework to enhance the resilience of IoT networks against malicious node attacks. By incorporating a multi-dimensional fuzzified trust assessment model that evaluates behavioural, energy, control message, and cooperative trust factors, the proposed approach effectively addresses the inherent security limitations of traditional RPL protocols. The use of fuzzy inference and adaptive trust thresholding enables accurate malicious node detection under uncertain and dynamic network conditions, resulting in more reliable and secure routing decisions.

Extensive simulations conducted in the Contiki–Cooja environment demonstrate that the proposed fuzzy trust mechanism significantly improves Packet Delivery Ratio, reduces end-to-end delay, enhances throughput, and lowers power consumption when compared to existing RPL security schemes. The adaptive fuzzy thresholding and trust-based routing strategies effectively isolate malicious nodes while minimizing false detections and maintaining low overhead. Future work will focus on extending the proposed framework to handle more sophisticated and combined attack scenarios, as well as integrating lightweight cryptographic primitives with fuzzy trust management to further strengthen the security and scalability of RPL-based IoT networks in real-world deployments.

In addition, the proposed approach lays a foundation for intelligent and autonomous trust management in large-scale IoT systems by enabling nodes to make context-aware security decisions with minimal human intervention. The flexibility of fuzzy logic allows seamless adaptation to heterogeneous device capabilities and dynamic network conditions, making the framework suitable for diverse IoT applications such as smart cities, healthcare monitoring, and industrial automation. By supporting distributed trust computation and localized decision-making, the framework reduces dependency on centralized control and improves fault tolerance. This adaptability and scalability ensure reliable and secure operation even as network size, traffic intensity, and threat complexity continue to grow.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

REFRENCES

[1] F. Azzedin, "Mitigating denial of service attacks in RPL-based IoT environments: trust-based approach," *IEEE Access*, vol. 11, pp. 129077-129089, 2023.

[2] N. Alfriehat, M. Anbar, M. Aladaileh, I. Hasbullah, T. A. Shurbaji, S. Karuppayah, and A. Almomani, "RPL-based attack detection approaches in IoT networks: review and taxonomy," *Artif. Intell. Rev.*, vol. 57, no. 9, p. 248, 2024.

[3] P. P. Ioulianou and V. G. Vassilakis, "Denial-of-service attacks and countermeasures in the RPL-based Internet of Things," in *Proc. Int. Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems*, Cham: Springer, pp. 374-390, 2019.

[4] D. Paganraj and M. Chelliah, "DE2RA-RPL: detection and elimination of resource-related attacks in IoT RPL-based protocol," *J. Supercomput.*, vol. 80, no. 15, pp. 22397-22427, 2024.

[5] H. Albinali and F. Azzedin, "Towards RPL attacks and mitigation taxonomy: systematic literature review approach," *IEEE Trans. Netw. Serv. Manag.*, 2024.

[6] Adarbah, Haitham Y., Mostafa Farhadi Moghadam, Rolou Lyn Rodriguez Maata, Amirhossein Mohajerzadeh, and Ali H. Al-Badi. "Security challenges of selective forwarding attack and design a secure ECDH-based authentication protocol to improve RPL security." IEEE Access 11 (2022): 11268-11280.

[7] S. Alsukayti and M. Alreshoodi, "RPL-based IoT networks under simple and complex routing security attacks: an experimental study," *Appl. Sci.*, vol. 13, no. 8, p. 4878, 2023.

[8] H. Mosa, A. Saleh, and M. Alkasassbeh, "RPL routing attacks detection for IoT networks using machine learning," in *Proc. Int. Jordanian Cybersecurity Conf. (IJCC)*, pp. 169-175, IEEE, 2024.

[9] S. Gonen, "A methodical examination of single and multi-attacker flood attacks using RPL-based approaches," *Comput. Ind. Eng.*, vol. 194, p. 110356, 2024.

[10] Wakili, Abubakar, and Sara Bakkali. "Enhancing IOT Routing Security and Efficiency: Towards Ai-Enabled Rpl Protocol." Available at SSRN 4907433 (2024).

[11] V. R. Rajasekar and S. Rajkumar, "A review of isolation attack mitigation mechanisms in RPL-based 6LoWPAN of Internet of Things," *Comput. Assist. Methods Eng. Sci.*, vol. 31, no. 3, 2024.

[12] M. Rouissat, M. Belkheir, I. S. Alsukayti, and A. Mokaddem, "A lightweight mitigation approach against a new inundation attack in RPL-based IoT networks," *Appl. Sci.*, vol. 13, no. 18, p. 10366, 2023.

[13] T. A. Alamiedy, M. F. R. Anbar, B. Belaton, A. H. Kabla, and B. H. Khudayer, "Ensemble feature selection approach for detecting denial of service attacks in RPL networks," in *Proc. 3rd Int. Conf. Advances in Cyber Security (ACeS)*, Penang, Malaysia, pp. 340-360, Springer, 2021.

[14] O. Bang, U. P. Rao, P. Kaliyar, and M. Conti, "Assessment of routing attacks and mitigation techniques with RPL control messages: a survey," *ACM Comput. Surv. (CSUR)*, vol. 55, no. 2, pp. 1-36, 2022.

[15] Kannan, M. Selvi, S. V. N. Santhosh Kumar, K. Thangaramya, and S. Shalini, "Machine learning-based intelligent RPL attack detection system for IoT networks," in *Advanced Machine Learning with Evolutionary and Metaheuristic Techniques*, pp. 241-256, Singapore: Springer Nature, 2024.

[16] K. Sridhar, B. A. Kumar, S. A. Devi, V. P. Raju, A. Soni, P. Singh, and S. S. Deore, "Enhancing security in IoT networks through RDAD for attack detection in RPL-enabled environments," *SN Comput. Sci.*, vol. 5, no. 7, p. 864, 2024.

[17] X. Wang, W. Yang, C. Hou, and H. Luo, "Routing attack and detection methods in the RPL-based Internet of Things," in *Proc. Int. Conf. Cyber-Enabled Distributed Comput. Knowl. Discovery (CyberC)*, pp. 127-130, IEEE, 2024.

[18] K. Ahmadi and R. Javidan, "A novel RPL defense mechanism based on trust and deep learning for Internet of Things," *J. Supercomput.*, pp. 1-25, 2024.

[19] S. Gonen, "A novel approach for RPL-based one and multi-attacker flood attack analysis," in *Proc. Int. Symp. Intell. Manuf. Serv. Syst.*, pp. 459-468, Singapore: Springer Nature, 2023.