International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I8P108

Volume 74 Issue 8, 109-135, August 2026

Original Article

MA-RL and WOA-Based Secure Routing: A Federated Learning Approach for Trust Evaluation and DoS Attack Mitigation in IoT Networks

M.N. Karuppusamy[1], N. Sasirekha[2]

[1,2]*Department of Computer Science, Vidyasagar College of Arts and Science, Udumalaipettai, Tamil Nadu, India.*

[1]*Corresponding Author : karuppusamy@vidyasagarcollege.org*

Received: 11 February 2026 Revised: 20 June 2026 Accepted: 03 July 2026 Published: 29 August 2026

Abstract - *The growing size and sophistication of the Internet of Things (IoT) has brought up the issue of network security and routing efficiency, especially in unfriendly settings where Denial-of-Service (DoS) attacks are frtaent. Conventional trust-based routing algorithms are not very flexible and are not capable of adequately addressing these dynamic threats. This paper puts forward a well-constructed smart and secure routing architecture that incorporates Multi-Agent Reinforcement Learning (MA-RL), Whale Optimization Algorithm (WOA), and Federated Learning (FL) to carry out more sophisticated trust scoring and DoS attack early warning. The framework is designed in three central steps, namely: (1) dynamic trust by MA-RL on the basis of metrics such as Packet Forwarding Ratio (PFR), rewards/penalties, and Received Signal Strength Indicator (RSSI); (2) privacy-preserving DoS detection via FL-based decentralized anomaly detection; and (3) optimized secure path selection with the use of WOA, where there is trust, energy efficiency, and a low latency. Moreover, a predictive time-series model predicts degradation of trust, which enables malicious nodes to be isolated in advance. The experimental assessment of the simulated IoT settings during the DoS attacks proves considerable positive changes in the detection rate, routing speed, and network stability. The proposed model has a high potential of securing the next-generation IoT networks as it has an adaptive learning capacity which is scalable.*

Keywords - *IoT, Security, DoS attack detection, Federated Learning, Trust management, Whale Optimization Algorithm.*

1. Introduction

The Internet of Things (IoT) has revolutionized the way of computing in the modern world to provide real-time connectivity between billions of interconnected devices in industries like smart homes, healthcare, industrial automation, and smart transportation Irrespective of these developments, IoT networks are very susceptible in that they utilize open wireless channels, distributed architecture, and limited capabilities of the devices (Kolias et al., 2019, Sharma et al., 2020, Shirvani & Masdari, 2023). The Denial-of-Service (DoS) attacks are some of the most disruption-based security threats since they target to flood network resources, reduce performance, and undermine service availability (Adam et al., 2024, Li et al., 2024). The typical security mechanisms, such as cryptographic protocols and Intrusion Detection Systems (IDS) tend to be intensive in terms of computational power, which is incompatible with the low-power IoT devices (Kaliappan et al., 2024, Khan et al., 2025, Burange et al., 2025).

As a solution to this, machine learning-based anomaly detection and trust-based security models have become lightweight and viable alternatives. These frameworks evaluate the actions of nodes based on trust measures to identify and isolate rogue entities beforehand. In this paper, a new secure routing paradigm that incorporates Multi-Agent Reinforcement Learning (MA-RL) (Aravindan & Rajaram, 2024, Antonio & Maria-Dolores, 2022, Nguyen et al., 2025) and the Whale Optimization Algorithm (WOA) (Nadimi-Shahraki et al., 2023, Mohammed et al., 2019) and Federated Learning (FL) (Nguyen et al., 2021, Imteaj et al., 2021). The proposed secure routing architecture will combine Multi-Agent Reinforcement Learning (MA-RL), Federated Learning (FL), and the Whale Optimization Algorithm (WOA) to improve security of IoT network against Denial-of-Service (DoS) attacks.

Rapidly emerging Internet of Things (IoT) applications, like smart healthcare, industry automation, transportation, agriculture and intelligent surveillance, also put a growing demand on secure, reliable and energy-efficient communication. The distributed and resource-constrained nature of the IoT networks makes them very susceptible to cyber threats such as DoS, selective forwarding, malicious

routing and trust manipulation attacks. These attacks impact on the delivery of packets, communication latency, energy usage and overall network stability.

Current approaches to securing Internet of Things (IoT) systems are primarily based on static trust models, centralized Intrusion Detection Systems (IDS), and traditional routing techniques, which are not suitable for dynamic attack environments. Static trust models cannot cope with the dynamically changing behaviour of nodes, and centralized detection models suffer from problems of scale, communication load and single-point failures. Furthermore, traditional routing protocols do not take into account trust, energy efficiency, attack resilience and delay, causing packet loss, increased latency, energy depletion and delayed attack mitigation.

While there have been recent advances in machine learning and optimization techniques for security in IoT, there are still some limitations in the current approaches, such as centralized data dependency, leakage of privacy, limited adaptability to new attacks, and inefficient routing optimization. While Federated Learning (FL) enables decentralized and privacy-preserving learning, current FL-based solutions often lack adaptively evaluating trustworthiness and optimizing routing securely. Likewise, optimization-based routing techniques do not give intelligent trust learning and attack prediction for proactive attacks.

Keeping these limitations in mind, the purpose of this research is to present an integrated secure routing framework based on Multi-Agent Reinforcement Learning (MA-RL), Federated Learning (FL), and Whale Optimization Algorithm (WOA) for adaptive trust evaluation, privacy-preserving DoS attack detection, predictive malicious node identification and multi-objective secure routing optimization. The framework's goal is to enhance the ability to resist attacks, maintain reliable routing, scalability, save energy, and communicate efficiently in dynamic IoT environments while using minimal resources and operating in a lightweight manner.

At the initial stage, MA-RL is used to evaluate dynamic trust among nodes, and each node calculates trust scores according to the main behavioral metrics, including Packet Forwarding Ratio (PFR), incentive-based rewards, penalty systems and Received Signal Strength Indicator (RSSI). Those nodes that behave consistently and cooperatively are rewarded, and those that engage in misrouting or packet dropping are penalized and gradually alienated by the network. This decentralized system of learning has the advantage of allowing every agent to dynamically judge the other nodes and conduct trust-based routing choices.

At the second stage, a privacy-sensitive anomaly detection system on Federated Learning is proposed. In this case, the IoT nodes are used to locally train lightweight LSTM or Transformer-based models with trust-related features, without dealing with raw data, and thus preserve the privacy of data. With the Federated Averaging (FedAvg) method, it is only the model parameters that are aggregated at a central server and are used to enhance global detection ability. A time-series-based forecasting model is also included to forecast the future values of trust in nodes, helping the system to preventively detect and remove the nodes that may become malicious in the coming time.

In the third stage, secure and efficient routing is used through the application of the Whale Optimization Algorithm (WOA). WOA bases its path selection based on the parameters of node reliability, remaining energy and the communication latency. As part of its exploration, exploitation, and convergence phases, WOA dynamically modifies the routing path to circumvent attack-compromised nodes to ensure network performance even when there is an attack. The framework provides an energy-efficient and resilient solution to the problem of an IoT network susceptible to DoS threats through the combination of MA-RL-based trust evaluation, FL-based anomaly detection and trust forecasting, and WOA-optimized path selection.

The rest of the paper will be structured in the following way: Section 2 is the related work, Section 3 will be the proposed methodology, and Section 4 is about the simulation results and the concluding section of the paper.

1.1. Research Problem

The Internet of Things (IoT) environment is rapidly growing and making securing distributed and resource-limited networks increasingly challenging from the perspective of the growing sophistication of cyber threats like Denial-of-Service (DoS) attacks, selective forwarding and malicious routing manipulation. Static trust computation models and centralized Intrusion Detection Systems (IDS) are not suitable for large-scale and highly dynamic IoT deployments since the majority of them are conventional security approaches. Static trust models are unable to dynamically adapt to the behavior of nodes, allowing malicious nodes to take advantage of temporary trust conditions before they are detected. In a similar manner, centralized attack detection methods result in single point failures, high computational load and communication overhead because of the regular transfer of monitoring information to the centralized servers.

The traditional routing protocols also have poor path selection, congestion, high latency and energy imbalance under adversarial conditions. Also, current trust management frameworks are not intelligent and fail to predict the degradation of trust or the appearance of new attack behaviour, causing an attack to be detected after it has occurred and network reliability to be undercut. All of these constraints combine to diminish the scalability, adaptability and resilience of IoT security solutions in live environments

that are hostile. Hence, an intelligent, decentralized, adaptive and light-weight security solution which can dynamically assess the level of trust, identifies new attack types, maintains privacy and optimise secure routing in large-scale IoT networks is highly needed.

1.2. Contribution of the Proposed Framework

The main contribution of this work is the development of a unified hybrid secure routing framework that combines Multi-Agent Reinforcement Learning (MA-RL), Federated Learning (FL), and Whale Optimization Algorithm (WOA) to enable adaptive trust evaluation, DoS attack detection and secure routing optimization with multiple objectives in a dynamic IoT environment. The proposed framework tackles decentralized trust learning, attack resilience, routing efficiency, scalability, and reduction in communication overhead in one intelligent architecture, unlike the traditional standalone trust and routing approaches.

1.3. The Novelty Concern of the Proposed Work

The novelty of the proposed work is that Multi-Agent Reinforcement Learning (MA-RL), Federated Learning (FL), and Whale Optimization Algorithm (WOA) are all combined in an integrated secure routing framework in the context of the Internet of Things (IoT). Existing approaches to security in the IoT have been largely based on isolated trust assessment, centralized intrusion detection, and routing mechanisms based on optimization techniques, without providing any ability to handle dynamic attacks, communication overhead, scalability, privacy preservation, and adaptive routing optimization simultaneously.

The proposed framework addresses these limitations by integrating the strengths of MA-RL, FL and WOA. The MA-RL component provides adaptive and decentralized trust evaluation based on nodes' behavior learning based on packet forwarding success rate, reliability of communication and the participation in attacks over time. In contrast to the static trust models, MA-RL dynamically adjusts trust value based on the changing environment in the network and the developing cyberattacks, thereby enhancing attack resilience and enhancing routing reliability.

The Federated Learning part improves privacy-friendly collaborative anomaly detection by letting IoT nodes train local models without sharing the raw data of their communications. This distributed learning method reduces communication overhead, avoids an over-reliance on a central server, makes the system more scalable, and increases the effectiveness of detecting an attack in distributed IoT systems.

The Whale Optimization Algorithm (WOA) component is used to carry out intelligent MO routing optimization, which is designed to choose highly trusted communication paths with the minimum energy cost and least delay. The routing mechanism dynamically adapts to the network changes, and it doesn't communicate through a compromised or unstable node. By utilizing these three in a combined approach, proactive attack mitigation, adaptive routing reconfiguration, decentralized trust learning, privacy preservation and secure routing optimization are all accomplished at once. Thus, the proposed one is more resilient against attacks, scalable, efficient in communication and stable in routing than the existing stand-alone IoT security and routing solutions.

2. Related Work

The problem of security in the Internet of Things (IoT) networks has recently become a burning issue of interest, especially because of the growing frequency and scope of Denial-of-Service (DoS) attacks. Such attacks compromise the stability and reliability of the IoT systems because of its limited computational and energy resources, which are usually abused by means of traffic flooding, packet dropping, or misrouting, which interfere with normal communication. Researchers have, in turn, investigated various forms of defense mechanisms, such as lightweight encryption, behavioral anomaly detection, trust-based evaluation models and optimization-enhanced secure routing protocols. Although the traditional cryptographic solutions are effective in the traditional network, they are likely to create excessive computational load that is not well-suited to the resource-constrained IoT devices. The following discusses some of notable works related to the security of the IoT environment.

Amid the IoT setups, Amer Aljaedi et al., (2025) suggested a light encryption algorithm that combines Discrete Wavelet Transform (DWT) and several chaotic maps to improve on the data security of the environment, at the same time ensuring computational efficiency of machines with limited resources. The federated learning-based trust assessment framework proposed by Wang et al., (2025) integrates security systems based on blockchains and the weighted model aggregation policy to guarantee decentralized, privacy-guaranteed, and robust security in IoT systems. Zhang, Y et al., (2024) introduced a lattice-cryptography-based Post-Quantum Identity-Based Signature (PQ-IDS) scheme as the IoT security framework, which is based on blockchain. The model will use a layered IoT architecture that will make it secure at the end-to-end when it comes to data security, privacy protection, and quantum resistance.

Mabodi, K. (2020) has suggested a hybrid security mechanism of AODV to protect gray hole attacks in IoT networks called MTISS-IoT that involves the use of cryptographic authentication and check node information. The method entails verification of node trust, route testing, attack detection and elimination of malicious nodes and simulation findings in NS-3 indicated high detection rate and low false positive and false negative rates. To allow dynamic and flexible authorization, (Putra, G. D et al., 2021) suggested decentralized attribute-based access control architecture of the

IoT that incorporates a Trust and Reputation System (TRS). It uses blockchain to achieve decentralization and side chains privately to store sensitive attributes information, and experimental results on an Ethereal test network showed that it was suieq to use in IoT settings.

To enhance the security of the internet of things through hardware-based protection and to give users of the IoT and cloud services vendors trust in this asset, (Faisal, M et al., 2020) suggested the implementation of a Trusted Platform Module (TPM) into the IoT computing systems. In the study, the known trusted computing schemes were examined, their limitations were determined, and it was shown that TPM-based IoT systems are more secure cryptographically and can overcome some important cybersecurity issues.

A zero-trust-based security architecture of the Power Internet of Things to facilitate large-scale device connectivity and share open services was suggested by Xiaojian, Z et al., 2021, which is based on the concept of continuous identity checking and dynamic access control. The methodology deals with the shortcomings of conventional border security concepts in power IoT settings. Khan, I. A et al., 2025 designed a contextual zero-trust intrusion detection architecture of the self-driving vehicles equipped with IoT technology that combines multi-source trust and reputation assessment with machine learning-based attack recognition. The framework uses crawler and observer modules to increase the objective assessment of trust and was shown to be highly accurate in detection in Car Hacking and ToN_IoT datasets.

Kumar, R et.al., 2025, suggested a dynamic trust management system based on AI and block chain that ensures the security of Industrial IoT. The solution uses trust ranking by machine learning and authentication of private block chains to reduce significant attacks as well as enhance system performance, scalability, and latency. Burange, A. W et al., 2025 came up with a trust-based IoT routing security model, which incorporates node behavior, reputation, and historical performance to improve the reliability and resilience of the network to routing attacks. The simulation results showed that it was very accurate in detection and mitigates attacks like wormhole, Sybil and rank, and still consumes less energy and is lightweight.

Besides the above, another group of authors have also talked about the security of the IoT environment (Kamble et al., 2025, Naghibi et al., 2025, Zheng et al., 202, Farhat et al., 2025, Li et al., 2025).

2.1. Research Gap

Although the IoT networks continue to be advanced to resist Denial-of-Service (DoS) attacks, scalability, adaptability, and efficiency are still challenging. The solutions that are currently available (lightweight encryption, IDS, trust models, and secure routing) have limitations: lightweight encryption continues to stress low-power equipment, post-quantum cryptography introduces latency, and machine learning-based IDS need large labeled datasets and central processing, which introduces vulnerabilities. Federated Learning (FL) enhances privacy, yet is not flexible enough to meet changing threats. Systems of trust, such as fuzzy logic and Bayesian models, have a hard time with adaptive attackers, and blockchain-based trust management consumes resources.

The secure routing is frequently not dynamic, and the hybrid key management is also not dynamic in updating the paths. The conventional optimization techniques are not flexible in the face of sudden modifications of attacks. In order to address these challenges, this work suggests a Secure Routing Framework that will involve Multi-Agent Reinforcement Learning (MA-RL), Whale Optimization Algorithm (WOA), and FL-based trust evaluation. FL allows the use of LSTM/Transformer models to detect anomalies that could be associated with privacy and the detection of emerging DoS patterns. MA-RL dynamically routes around trusted assessment in real-time, enhancing attack resilience. The routing optimization of WOA is based on choosing stable and high-trust nodes based on the trust, energy, and latency and is continuously adjusted to respond to misbehavior. This combined solution provides better security, efficiency, and scalability, which makes the IoT networks less vulnerable to DoS attacks.

2.2. Advanced Threat Model

Due to its distributed network, wireless communication media, and resource-limited devices, IoT networks are susceptible to different types of routing and communication attacks. Besides DoS attacks, malicious nodes can execute multiple advanced attacks that can affect the stability of the routing function, influence the trust evaluation process, increase the communication overhead, and decrease network reliability. Therefore, the design of the proposed framework takes into account various advanced attack scenarios to enhance the attack resistance and secure communication in dynamic IoT environments.

A sinkhole attack is a type of attack in which a malicious node pretends to be the best or shortest route to another node to lure traffic into its direction. Neighbor nodes choose the malicious node as an intermediate node, and the attacker can modify, drop, or observe the packets that traverse the compromised node. Likewise, Sybil attacks rely on a malicious node generating false identities in the network to manipulate the trust calculation, routing choices, and communication protocols in collaborative networks. False entities can “fool” other nodes and lead to a reduction in overall network stability.

Wormhole attacks involve two malicious nodes that establish a low-latency path between two remote nodes in the

network, and then replay routing messages over the path. It can give the illusion of shorter routing paths and interfere with the usual network topology. Replay attacks are when a routing or trust packet is maliciously captured and re-transmitted at a later time to form outdated or misleading routing information.

Another type of attack is selective forwarding, where malicious nodes randomly drop a portion of packets while forwarding the rest to the rest of the network to hide the attack, since only a portion of packets are dropped. Unlike a mirror attack, blackhole attacks simply delete and ignore all traffic from the other host, resulting in a heavy loss of packets and a total loss of communications. Jamming attacks cause radio interference signals to be sent out into the wireless communication channels, which affects signal quality, requires more packet retransmissions, and negatively impacts wireless communication performance.

This proposed solution, based on the use of MA, RL and WOA, includes several defense mechanisms to counter these attacks. The MA-RL-based trust evaluation continuously tracks the node behavior and automatically identifies any abnormal variation of trust due to malicious forwarding or identity manipulation, or packet-dropping activities in the network. The Federated Learning-based anomaly detection algorithm is able to detect distributed traffic anomalies and suspicious communication patterns without exposing any data from the nodes, which enhances the accuracy of attack detection while also maintaining privacy. Besides, the Whale Optimization Algorithm (WOA)-based routing mechanism eliminates the compromised and low-trust nodes through dynamic selection of trustworthy, stable, and energy-efficient routing paths. The proposed architecture enhances the resilience of the system to various complex IoT attack scenarios using adaptive trust learning, decentralized anomaly detection, and intelligent routing optimization.

3. Proposed Work: TFL-WOA-SR

The proposed framework aims to improve IoT network security by integrating Multi-Agent Reinforcement Learning (MA-RL), Federated Learning (FL), and the Whale Optimization Algorithm (WOA) to enable secure and efficient routing. Central to the model is a dynamic trust evaluation system powered by MA-RL, which assesses node behavior using metrics such as Packet Forwarding Ratio (PFR), incentives and penalties, and Received Signal Strength Indicator (RSSI). To enhance the detection of Denial-of-Service (DoS) attacks, FL is employed for decentralized and privacy-preserving anomaly detection, addressing vulnerabilities linked to centralize processing. Secure routing is further optimized through WOA, which selects the most reliable and efficient communication paths. The proposed MA-RL framework assumes that each IoT node acts as an intelligent learning agent and is constantly monitoring the activities of its neighboring nodes, dynamically adjusting its trust levels based on the communication performance. In the MA-RL model, the state space is composed of critical network parameters, such as Packet Forwarding Ratio (PFR), Received Signal Strength Indicator (RSSI), residual energy, queue condition and communication delay. These parameters allow the learning agent to continually assess the reliability of each node, the stability of the communications, and the performance of the routing under dynamic attack.

The parameters that are used to define the MA-RL state representation include forwarding behavior, energy available, communication quality, and congestion. The Packet Forwarding Ratio (PFR) shows the reliability of node forwarding; RSSI is the stability of the signal; residual energy is used to measure the sustainability of the node; queue condition reflects the status of congestion; and communication delay reflects the efficiency of communication transmission. These parameters enable the proposed framework to effectively separate cooperative nodes from malicious and unstable nodes.

The action space of the MA-RL model consists of a variety of routing-related operations, including normal packet forwarding, malicious node isolation, secure rerouting and updating of the trust value. Nets are dynamic, sense-oriented, with nodes dynamically choosing actions based on current trust conditions and observed communication behavior in the network. Cooperative forwarding actions will increase the trustworthiness of the nodes, while suspicious activities like dropping packets, selective forwarding, or routing manipulation will decrease the trustworthiness of the nodes by applying penalties.

The reward mechanism aims to promote reliable communication and deter bad behavior. Successful packet forwarding, stable communication and trustworthy routing participation are rewarded with positive rewards. The packet loss, communication disturbance, abnormal forwarding and attack participation are assigned a negative reward or penalty. The reward weighting parameters dictate the weight that forwarded reliability, communication stability, and maliciousness have on trust adaptation. This adaptive learning process allows the network to progressively detect malicious nodes and enhance the reliability of the routing in the dynamic attack scenario.

For better reproducibility, hyperparameter values were explicitly specified for the implementation of MA-RL and WOA. The learning rate in MA-RL was obtained by setting it to 0.01 to guarantee the stable convergence of trust during training. Immediate and future routing rewards were balanced by using a discount factor of 0.85. To ensure learning stability, the replay memory size was set to 5000, and to efficiently update the model, the batch size was configured to 32. To maintain a balance between exploration and exploitation while learning from adaptively chosen trust, the exploration probability was gradually decreased from 0.1 to 0.01.

During the WOA-based routing optimization process, each whale is a candidate routing path. The routing fitness evaluation takes into account the trustworthiness, the residual energy, the communication delay and the routing stability to find out the paths of communication that are secure and energy efficient. To obtain stable routing convergence under a dynamic network condition, the whale population size was changed between 10 and 50 and optimized 100 times.

3.1. IoT Network Model Assumptions

- 'N' IoT nodes that will be used in the network are deployed in an ad-hoc manner.
- Each node has limited computing power, and it is energy-constrained, so energy efficiency is a major consideration.
- Communication is based on multi-hop routing as intermediate nodes are used to process packets in their direction to the target.
- Each node has a trust score, which is indicative of its past reliability.

3.2. Security Assumptions

- The IoT network can be considered susceptible to DoS attacks, in which malicious nodes are aimed at obstructing communication.
- Attackers can act in an ordinary manner at the start to enable them not to be detected by the trust system before they cause attacks.
- Nodes share information that is related to trust periodically, and maintain privacy by not sharing raw data.
- The evaluation of trust is done in a decentralized way by exploiting Federated Learning.

3.3. Assumptions of Communication and Routing

- Some of the characteristics of nodes include a limited range of transmission, which requires multi-hop communication routes.
- Every node has a local trust record, which is founded on immediate observations and previous encounters.
- The router choices are shaped by several parameters, among them, Packet Forwarding Ratio (PFR): This parameter measures the stability of the node to forward packets in the right direction. Rewards and Penalties: Recognizes positive conduct and punishes ill intentions. Received Signal Strength Indicator (RSSI): This enables the transmission power to be adjusted dynamically depending on the distance of the node.
- The suggested scheme facilitates the security of the IoT by identifying DoS attacks and predicting further trust behavior, as well as optimizing path routing in three important stages.
    - Evaluation of trust with Multi-Agent Reinforcement Learning (MA-RL).
    - DoS Attack Detection Federated Learning.
    - Secure Routing based on Whale Optimization Algorithm (WOA).

Phase 1: Trust Evaluation Using Multi-Agent Reinforcement Learning (MA-RL)

In an IoT-based network, sensor nodes will perform the duty of forwarding packets, and their reliability can be evaluated with the Packet Forwarding Ratio (PFR). The PFR at sensor node SNi at time t, A, is obtained by evaluating sensor node SNj at time t, B, as shown below:

$$PFR(SNi, SNj, t) = \frac{P_{forwarded}(SNj,t)}{P_{received}(SNi,t)} \quad (1)$$

Where $P_{forwarded}(SNj, t)$ represents the number of packets successfully forwarded by '*SNj'* and $P_{received}(SNi, t)$ denotes the number of packets received by '*SNj'*. A low PFR, specifically when $PFR\ (SNi,SNj,t) < PFR_{thresh,}$ indicates possible malicious behavior, such as selective packet drops, which may suggest the presence of a DoS attack. To incentive cooperative nodes and penalize malicious behavior, an incentive mechanism is employed. The incentive score of a node *'SNj'* at time *'t'* is updated as:

$$I(SNi, SNj, t) = I(SNi, SNj, t-1) + \gamma_1 PFR(SNi, SNj, t) - \gamma_2 P_{misroute}(SNj, t) \quad (2)$$

Where $P_{misroute}$ (SNj,t) denotes the number of misrouted packets detected for SNj and γ_1 *and* γ_2 are weight factors regulating rewards and penalties. Malicious nodes engaging in misrouting or packet dropping experience a decline in incentives, whereas well-behaved nodes accumulate higher incentives over time, prioritizing them for routing. A penalty mechanism is also incorporated to degrade the trustworthiness of malicious nodes. The penalty score is computed as:

$$Penalty(SNi, SNj, t) = Penalty(SNi, SNj, t-1) + \gamma_1(1 - PFR(SNi, SNj, t) - \gamma_2 P_{misroute}(SNj, t) + \gamma_{3P_{Dos}(SN,t)} \quad (3)$$

Where P_{DoS}(SNj,t) represents detected DoS attack attempts, and γ1,γ2 and γ3are weight factors associated with packet drops, misrouting, and detected DoS attacks.

A node accumulating excessive penalties, such that $Penalty\ (SNi, SNj,t) > Penalty_{thresh}$, is eventually isolated from routing. Another crucial metric for trust evaluation is the Received Signal Strength Indicator (RSSI), which measures link stability. The RSSI of a node SNj at time t is given by:

$$RSSI(SNi, SNj, t) = RSSI_{initial} - \vartheta d(SNi, SNj, t) + \delta I_{noise}(SN_j, t) \quad (4)$$

Where $RSSI_{initial}$ is the initial signal strength, d (SN_i, SN_j,t) represents the distance between SN_i and SN_j, and I_{noise}(SNj,t) captures interference and noise affecting the node. The parameters η and δ regulate the impact of distance and noise on signal attenuation. Malicious nodes may manipulate RSSI values to perform jamming or spoofing attacks, disrupting network stability.

Multi-Agent Reinforcement Learning (MA-RL) would be used in the proposed system to dynamically assess and revise the trust scores of the IoT nodes in accordance with their actions. The MA-RL assumes that each of the IoT nodes is a separate agent, which learns through its interaction with the surrounding nodes and the environment of the network as well. Each agent (node) aims to maximize its credibility, at the same time as being energy efficient and reducing delays in the data transmission. Markov Decision Process (MDP) forms the basis of this mechanism of learning, and each node refreshes its trust score sequentially according to the reward and penalty that is faced by the environment. The MA-RL framework has major elements like the state Sn that has the trust score T(n), the Packet Forwarding Ratio (PFR) PER(n), the incentive score I(n), the penalty score Penalty(n) and the received signal strength indicator RSSI(n) that take the form:

$$S_n = \{T(n), PFR(n), I(n), Penality(n), RSSI\ (n)\} \quad (5)$$

An action taken by a node is based on its learned policy π, and it involves cooperative packet forwarding, selective forwarding, dropping packets or misreporting trust values. The reward function is used to encourage cooperative behavior and discourage misbehavior. It is calculated as,

$$R_n(t) = \beta_1.PFR(n) + \beta_2.I(n) - \beta_3.Penality(n) + \beta_4.RSSI(n) \quad (6)$$

Where β_1, β_2, β_3, and β_4 are weight factors influencing the reward. The policy π is learned using reinforcement learning techniques such as Q-learning or Deep Q Networks (DQN) and aims to maximize cumulative rewards. The Q-value update follows the equation.

$$Q(S_n, A_n) = Q(S_n, A_n) + \alpha[R_n + \gamma(s'_n, A'_n) - Q(S_n, A_n)] \quad (7)$$

In which α is the learning rate, γ is the discount factor, and S_n, $A_n$denote the successive state-action pair. MA-RL has a learning process that starts by initializing each IoT node with a neutral policy and an initial trust score. The nodes then monitor their states, which are PFR, incentives, penalties and RSSI, and to take an action based on what they have learned as policy. This action is chosen, and it impacts on the network, which affects the trust score of the node. A reward is then obtained as a result of the behavior of the node, and the trust score T (n) is updated as:

$$T(n) = \alpha_1.PFR(n) + \alpha_2.I(n) + \alpha_3.Penality(n) + \alpha_4.RSSI(n) \quad (8)$$

The reinforcement learning techniques are also employed to update the Q-value to optimize the decision-making process by the node. With time, each node continues to refine its policy in order to achieve maximum reward and enhance trustworthiness, and this process recurs until it changes to react to dynamic network conditions. Trust evaluation with the help of MA-RL has a number of benefits. It allows decentralized decision-making, and nodes can assess trust independently based on local experience without depending on a centralized authority. This increases scalability and minimizes overhead communication. The flexibility of MA-RL to dynamic environments means that the trust assessment is dynamic and can best handle dynamics in node behavior and new security risks. Also, MA-RL is more resilient to attacks, including the case of trust deception, in which malicious nodes seek to manipulate the trust values. The malicious nodes are eventually isolated, as the rewards are reduced through penalties.

Moreover, MA-RL maximizes trust-based routing, which means the nodes will be informed to choose the most trustful and energy-efficient paths that will enhance the overall security and performance of the network. Using MA-RL to evaluate trust, the IoT network will dynamically respond to changing threats and block malicious activities and make sure that only high-trust nodes are involved in the transmission of secure data. The strategy would improve the detection of DoS attacks, secure routing, and general resilience of the IoT network.

Phase 2: Federated Learning DoS attack detection

In the proposed framework, phase 2 is dedicated to the Federated Learning (FL)-based Denial-of-Service (DoS) attack detection, so that trust estimation and anomaly detection is done in a decentralized and privacy-conscious way. Since the IoT network is distributed, similar to the case of IoT networks with nodes constantly exchanging data and sending packets, identifying an operating malicious device, such as DoS attacks, is essential to network integrity. Centralized detection mechanisms that have been traditionally used cannot be implemented because of bandwidth limitations, privacy, and points of failure. In order to address these constraints, Federated Learning (FL) will be used, which will allow the nodes to jointly train an anomaly detection model without distributing raw trust data. It can be separated into two major steps, i.e., local training at the nodes of the IoT and federated training at the FL server. The second step is training local models by the IoT nodes:

Step 2.1. Training

The model to detect anomalies is trained locally at each node n in N using the historical trust data, which contains the

following features: the Packet Forwarding Ratio (PFR), incentive score, penalty score, and Received Signal Strength Indicator (RSSI). The nodes also update their local model parameters, rather than sending raw data to a central server. Most anomaly detection models are built around the principles of the deep learning architecture, such as Long Short-Term Memory (LSTM) networks or Transformers, which are effective in temporal trust patterns and detecting malicious deviations. The training process for each node can be represented as follows:

$$\Delta W_n = \text{Train}(D_n, W_n) \quad (9)$$

Where:

- ΔW_n is the local model update (parameter adjustments) for node n.
- D_n represents the locally collected trust dataset at node n.
- W_n is the initial model weight before training.
- Train () is the training function that updates the model based on loss minimization.

Each node updates its model by minimizing a local loss function L_n, typically formulated as:

$$L_n = \frac{1}{|D_n|} \sum_{(x,y) D_n} \text{LOSS}(f(x; W_n), y) \quad (10)$$

Where:

- $f(x; W_n)$ is the model's predicted trust score for an input xxx.
- y is the actual trust label.
- Loss () is a function, such as cross-entropy loss or Mean Squared Error (MSE), for anomaly detection.

Once local training is completed, each node computes its model update. ΔW_n and sends it to the FL server instead of sharing raw trust data. This enhances privacy and reduces network congestion, as only parameter updates are exchanged.

Step 2.2. Federated Aggregation at the FL Server

After collecting model updates from multiple IoT nodes, the FL server aggregates them to improve the global model. This aggregation process is performed using Federated Averaging (FedAvg)**,** which combines all local updates as follows:

$$W_{global} = \frac{1}{|N|} \sum_{n \in N} \Delta W_n \quad (11)$$

Where:

- W_{global} represents the updated global anomaly detection model.
- |N| is the total number of participating IoT nodes.
- ΔW_n the local model update from node n.

By averaging these local updates, the global model learns collective network behavior while preserving the privacy of individual nodes. The server then distributes this refined global model back to all IoT nodes, equipping them with enhanced anomaly detection capabilities.

Step 2.3. DoS Attack Detection & Malicious Node Isolation

Each IoT node integrates the updated global model into its local anomaly detection framework. When a new data instance (trust evaluation report) arrives, the node applies the trained model to classify whether the behavior is normal or indicative of a DoS attack. The classification decision is made using:

$$\tilde{y} = f(x; W_{global}) \quad (12)$$

Where:

- $\tilde{\mathbf{y}}$ is the predicted label (normal or malicious).
- $f(x; W_{global})$ is the anomaly detection function using the global model.

If an IoT node n is identified as malicious (i.e., $\tilde{\mathbf{y}}$ indicates an attack), the system isolates the node from routing paths to prevent further disruption. This is enforced using:

$$Routing\ Table = \{n\}, if\ f(x; W_{global}) = malicious \quad (13)$$

where:

- The Routing Table maintains paths for secure packet forwarding.
- The malicious node n is removed from all available routing paths.

Phase 3: Whale Optimization Algorithm (WOA) for Secure Routing

Although Federated Learning (FL)-based DoS attack identification can successfully detect and isolate the bad nodes, routing is not optimized, and hence, the Whale Optimization Algorithm (WOA)-based step of secure routing can be very important. After the identification and elimination of malicious nodes, the network will still have to identify the optimal and safest path across the network of the remaining trusted nodes. This necessitates a routing strategy, which puts into consideration various variables, including, but not limited to, trustworthiness, energy efficiency, and end-to-end delay, so that the choice of paths that optimize network performance is made. IoT networks are very dynamic in nature, as nodes may be added, removed, or change their behavior. FL-based detection uses the trust data of the past and the pre-trained models, which does not automatically identify new patterns of attacks or malicious behavior with sub-text. This flexibility provides assistance in countering threats caused by unidentified attacks or those that are continuously changing and adapting, as well as balance in the use of network

resources. Moreover, WOA also avoids the overloading of some nodes, spreading traffic effectively, thus increasing the life expectancy of the network. Because FL models need regular retraining to fit emerging attack patterns, only an FL-based detection can create gaps in real-time security. WFWA removes this drawback by dynamically adjusting to the existing network conditions without having to retrain. In addition, the WOA-based routing offers a more flexible and scalable method than the static or semi-adaptive routing mechanisms, as the network size of the IoT is scaled.

Step 3.1. Initialize WOA Parameters

To begin the optimization process, WOA initializes a population of whales, where each whale represents a candidate routing path in the IoT network. The algorithm starts by:

- Defining the whale population P as the set of candidate routing paths, where each path is represented as Xi.
- Setting the maximum number of iterations, I_{max}, to control the convergence speed of WOA.
- Initializing the positions of the whales (i.e., the candidate paths), denoted as:

$$X = X_1 + X_2 + X_3 \ldots\ldots + X_n \quad (14)$$

where each Xi represents a potential routing path in the network. These initial paths are randomly selected or determined based on heuristic rules.

Step 3.2. Compute Fitness for Each Routing Path

To evaluate the quality of each candidate path, a fitness function F (Xi) is computed based on three key factors:

$$F(X_i) = W_1.T(X_i) + W_2.E(X_i) + W_3.D(X_i) \quad (15)$$

where:

- T(Xi) is the trust score of the path, ensuring that only trustworthy nodes participate in routing.
- E(Xi) represents the energy efficiency, prioritizing paths with nodes that have sufficient residual energy.
- D(Xi) is the end-to-end delay, minimizing latency in data transmission.
- w1, w2, and w3are weight factors that balance the impact of trust, energy, and delay on the fitness function.

Each routing path is evaluated based on this fitness function, and the path with the highest fitness value is selected as the best path X∗(t) for the current iteration:

$$X*(t) = arg\ max\ F(Xi) \quad (16)$$

This ensures that the best path is trustworthy, energy-efficient, and has low delay.

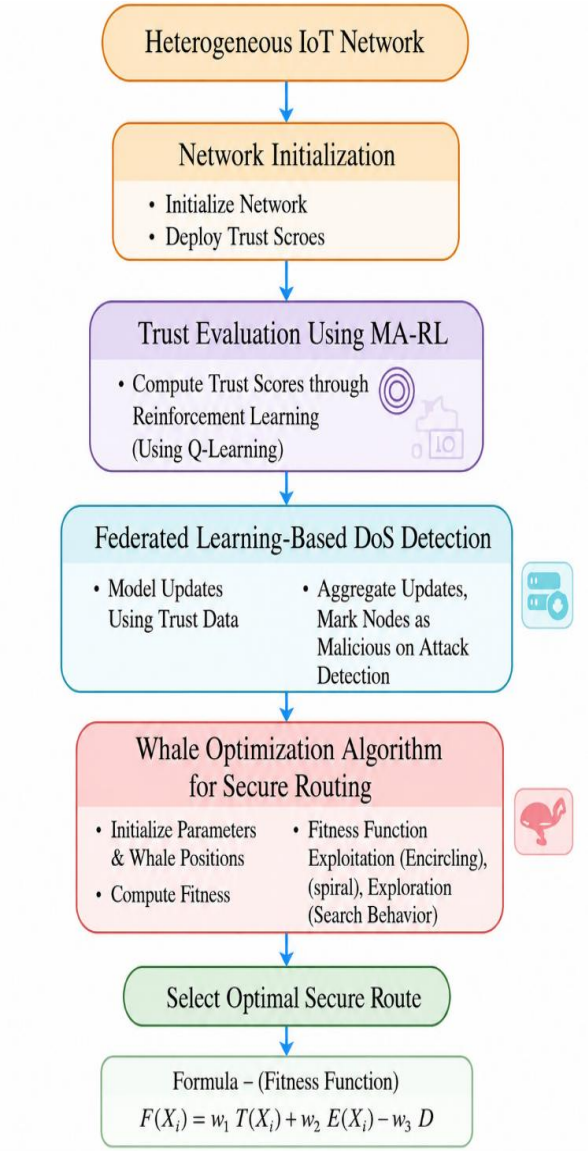

Fig. 1 The architecture diagram of the proposed model

Step 3.3. Encircling Prey (Nodes Move toward Best Route)

Once the best path X∗(t) is identified, other candidate paths adjust their positions to move closer to this optimal path. This mimics the whale encircling behavior, where whales move toward their prey. The position of each path is updated as:

$$X(t+1) = X*(t) - A \cdot D \quad (17)$$

where:

- A is the adaptive coefficient controlling exploration vs. exploitation.
- D is the distance between the current path and the best path, computed as:

$$D = | C \cdot X*(t) - X(t) | \quad (18)$$

Here, C is a random coefficient that introduces variation, allowing paths to be dynamically adjusted. This step helps the network nodes to converge toward the optimal secure path.

Step 3.4. Bubble-Net Attacking (Exploitation Phase)

To further refine the routing path selection, WOA uses a spiral movement known as bubble-net attacking. This step simulates the spiral hunting technique of whales and is modeled using:

$$X(t+1) = D' \cdot e(b \cdot l) \cdot \cos(2\pi l) + X * (t) \quad (19)$$

Where:

- D' is the distance between the current candidate path and the best path.
- b is the logarithmic spiral coefficient, controlling the shape of the movement.
- l is a random number in the range [−1,1] ensuring stochasticity.

This phase exploits the best-found routing path by searching nearby paths that might have slightly better properties in terms of trust, energy, or delay.

Step 3.5. Search Behavior (Exploration Phase)

To avoid premature convergence and ensure the algorithm explores a diverse set of routing paths, WOA incorporates a search mechanism where candidate paths randomly explore new routes. The position update equation for this phase is:

$$X(t+1) = Xrand - A \cdot D \quad (20)$$

Where:

- X_{rand} is a randomly selected path from the search space.
- A and D control the exploration behavior.

This exploration diversifies the search space by considering new routing paths, preventing the algorithm from getting trapped in a local optimal.

Step 3.6. Select Optimal Secure Route

After I_{max} iterations, WOA converges to the best secure routing path, which is selected as the final routing path:

$$Xopt = \arg\max F(Xi) \quad (21)$$

This final path is chosen based on the highest fitness score and is used for secure data transmission. The following algorithm depicts the proposed work.

3.4. Federated Learning Challenges

However, Federated Learning (FL) presents several challenges in real-world IoT scenarios, such as data heterogeneity, client drift, communication limitations, and resource constraints. The proposed framework includes several mechanisms to overcome these challenges and enhance the scalability and stability of collaborative anomaly detection in dynamic IoT networks. One of the most significant difficulties in a distributed-based IoT system is data heterogeneity, where the trust data and traffic data generated from different IoT nodes are non-identically distributed (non-IID) due to the different types of devices, communication patterns, environmental conditions, and exposure to attacks.

For instance, sensors in the healthcare environment, those in the industrial IoT, or environmental monitoring nodes can have varying communication patterns and traffic characteristics. The proposed FL-based anomaly detection framework tackles it by aggregating and learning knowledge from several distributed heterogeneous IoT nodes, and enhancing the generalization capability of the overall anomaly detection model, through decentralized collaborative learning based on Federated Averaging (Fed Avg).

The drift of the client can happen if local models are trained independently by each node, with different local data and communication contexts. There can be some differences between local and global models due to local training behavior, asynchronous participation, and inconsistent node availability. The proposed framework periodically aggregates the local model updates and uploads them to the global FL server using adaptive aggregation mechanisms to reduce the drift of the clients. The continuous updating of the model facilitates consistency in learning and minimizes model divergence under dynamic network conditions.

Another key challenge in resource-constrained IoT environments is communication constraints due to the continuous exchange of models, which is known to consume bandwidth, communication overhead, and energy. The proposed framework brings in the benefit of having a partial client participation, light local training, reduced communication frequency and optional model compression techniques, which help in reducing the communication overhead. In each federated learning round, only some IoT nodes are involved, and local training models are lightweight LSTM or Transformer models that are suitable for low-power devices.

Besides, only model parameters and local updates are shared between the IoT nodes and the FL server, rather than the actual trust or traffic data. This decentralized communication method ensures privacy, reduces bandwidth usage, and enhances scalability in large-scale IoT deployments. In summary, the proposed FL framework is capable of supporting heterogeneous IoT data effectively, mitigating client drift, decreasing communication overhead, and enhancing collaborative attack detection performance in the presence of a dynamic network.

Algorithm 1. MA_RL_WOA_SecureRouting

```
Input:
N        ← Set of heterogeneous IoT nodes
P        ← Set of candidate routing paths
T(n)     ← Initial trust score of node n
E(n)     ← Residual energy of node n
D(n)     ← Communication delay of node n
w1, w2, w3 ← Weight factors for trust, energy, and delay
I_max    ← Maximum WOA iterations
FL_Model ← Federated Learning model for DoS attack detection
Output:
X_opt    ← Optimal secure routing path
Begin
    //-------------------------------------------------------
    // Step 1: Network Initialization
    //-------------------------------------------------------
    Initialize IoT network with nodes N
    Deploy nodes in an ad-hoc multi-hop topology
    For each node n ∈ N do
    Assign initial trust score T(n) based on historical data
    Initialize residual energy E(n)
    Initialize communication delay D(n)
    End For
    //-------------------------------------------------------
// Step 2: Trust Evaluation Using Multi-Agent Reinforcement Learning (MA-RL)
    //-------------------------------------------------------
    // Step 2.1: Compute Trust Metrics
    For each node n ∈ N do
    Compute PFR(n)   ← Packet Forwarding Ratio of node n
    Compute I(n)     ← Incentive score for cooperative behavior
    Compute Penalty(n) ← Penalty for untrustworthy actions
    Compute RSSI(n)  ← Received Signal Strength Indicator
        // Trust Score Calculation
    T(n) ← α1*PFR(n) + α2*I(n) - α3*Penalty(n) + α4*RSSI(n)
    End For
    // Step 2.2: MA-RL Trust Update
    For each node n ∈ N do
    Observe state S(n) ← [PFR(n), I(n), Penalty(n), RSSI(n)]
   Choose action A(n) using policy π (update trust or isolate node)
    Receive reward R(n) based on forwarding behavior
   Update policy π using reinforcement learning (e.g., Q-learning)
    End For
    //-------------------------------------------------------
// Step 3: Federated Learning-Based DoS Attack Detection
    //-------------------------------------------------------
    // Local Model Training
    For each node n ∈ N do
    Train a local anomaly detection model using trust-related data
    Compute model update ΔW_n
    Send ΔW_n to FL server
    End For
    // Federated Aggregation
    Aggregate global model:
    W_global ← (1 / |N|) * Σ ΔW_n
    Distribute W_global back to all nodes
    For each node n ∈ N do
    If FL_Model detects a DoS attack on node n, then
    Mark node n as malicious
    Remove node n from routing paths P
    End If
    End For
    //-------------------------------------------------------
    // Step 4: Whale Optimization Algorithm (WOA) for Secure Routing
    //-------------------------------------------------------
   // Step 4.1: Initialize WOA Parameters
   Initialize whale population with candidate paths P
   Set iteration counter t ← 0
   Initialize whale positions X = {X_1, X_2, ..., X_m}
   // Step 4.2: Compute Fitness of Each Candidate Path
   While t < I_max do
      For each path X_i ∈ P do
         Compute:
      F(X_i) ← w1*T(X_i) + w2*E(X_i) - w3*D(X_i)
      End For
      Select best path X_best(t) with highest fitness F(X_i)
      // Step 4.3: Encircling Prey (Exploitation)
      For each path X_i ∈ P do
         Update:
            D ← |C * X_best(t) - X_i|
            X_i ← X_best(t) - A * D
      End For
      // Step 4.4: Bubble-Net Attacking (Exploitation - Spiral)
      For each path X_i ∈ P do
         D' ← |X_best(t) - X_i|
         l  ← random number in [-1,1]
         X_i ← D' * exp(b*l) * cos(2π*l) + X_best(t)
      End For
      // Step 4.5: Search Behavior (Exploration)
      For each path X_i ∈ P do
         Choose a random path X_rand ∈ P
         D ← |C * X_rand - X_i|
         X_i ← X_rand - A * D
      End For
      Increment t ← t + 1
```

82. End While
83. //----------
84. // Step 4.6: Select Optimal Secure Route
85. //----------
86. X_opt ← argmax{ F(X_i) | X_i ∈ P }
87. Return X_opt
End Algorithm

4. Security Analysis

The proposed approach of secure routing based on MA-RL, Federated Learning (FL) and Whale Optimization Algorithm (WOA) significantly improves the security of IoT networks by implementing adaptive trust evaluation, decentralized anomaly detection and intelligent routing optimization. In contrast with the traditional methods that are based on static trust computation and centralized intrusion detection, the proposed framework is adaptable to different network conditions and attacks. By incorporating reinforcement learning, collaborative learning, and bio-inspired optimization, the system enhances its resilience against attacks, stability, communication efficiency, and privacy protection in dynamic IoT scenarios.

4.1. Trust Convergence Analysis

The proposed framework is based on a trust evaluation mechanism in which the IoT nodes keep track of the behavior of the surrounding nodes and dynamically adjust their trust value based on the reliability and forwarding behavior of the surrounding nodes. The nodes that cooperate by forwarding packets correctly and the communication channels between them gradually receive higher trust values, while the nodes that drop packets, misroute packets or disrupt communication between nodes receive penalties and their trust values decrease over time.

This adaptive trust mechanism allows the network to continuously observe the behavior of nodes and distinguish them from malicious nodes. A dynamic adaptation to changing attack conditions and node behaviors is implemented in the proposed framework, unlike static trust models. As malicious behavior continues to happen, the compromised nodes are increasingly distrustful of each other and are then excluded from routing participation, thus increasing the routing reliability and network stability. A decentralized trust evaluation system also decreases the reliance on centralized authorities, decreasing communication expenses and boosting scalability.

4.2. Detection of DoS attack

The proposed framework enhances the resistance to Denial-of-Service (DoS) attacks by combining the MA-RL-based trust learning with FL-based anomaly detection. The abnormal communication behaviors (such as packet forwarding ratio, routing consistency, incentive scores, and RSSI) are continuously monitored to detect malfunctions, including packet flooding, routing manipulation, and selective forwarding, carried out by malicious nodes.

Suspicious nodes start to receive penalties over time, and they become increasingly distrustful until they are not able to participate in routing, until they cause significant network disruption. Furthermore, the FL-based anomaly detection mechanism facilitates collusion-based anomaly detection among distributed IoT nodes without exchanging raw data. This distributed learning approach not only enhances the accuracy of attack detection but also ensures privacy and minimizes communication traffic.

The combination of adaptive trust learning by nodes and collaborative anomaly detection plays an important role in improving the ability of the system to detect and defend against malicious nodes in dynamic attack environments.

4.3. Secure Routing Analysis

The proposed framework integrates Whale Optimization Algorithm (WOA) into the secure routing, enhancing the reliability of communication and preventing compromised routing paths. Traditional routing protocols are primarily concerned with the shortest-path routing, and they do not take into consideration the trustworthiness, residual energy, congestion, or even the attack resilience. In the result, the malicious nodes could join the routing and interfere with the communication by dropping the packets or routing manipulation.

A routing mechanism based on WOA is proposed, which is used to optimize routing decisions based on parameters like trustworthiness, residual energy, communication delay, and network stability. The algorithm will keep looking for a communication path with reliable and energy-efficient nodes without involving any suspicious or low-trust nodes. This adaptive optimization allows route reconfiguration in case of the detection of malicious behavior or unstable communication.

The routing strategy also has better resistance against attacks like wormhole, blackhole, selective forwarding and sinkhole attacks. The framework ensures packets are delivered reliably, even with the loss of a node, as they lose trust and are not used in routing paths. Furthermore, the optimized routing approach reduces end-to-end delay by reducing congestion and retransmissions.

4.4. Privacy Preservation Analysis

The proposed framework maintains privacy by adopting Federated Learning (FL) based collaborative anomaly detection. The proposed approach is different from an IDS system with central learning, which requires raw traffic data to be transmitted to a central entity for learning, as IoT nodes will locally train anomaly detection models using their own trust and communication data. Model parameters and learning

updates are the only ones to be shared with the aggregation server.

This distributed learning approach helps to store critical network information safely while allowing for joint attack detection from multiple distributed IoT nodes. No raw data is sent, so there are significantly lower risks of communication overhead and privacy leakage. The distributed architecture of FL also addresses the centralized failure issues and enhances scalability for large-scale IoT deployments.

In summary, the proposed framework's adaptive trust learning, decentralized anomaly detection, and intelligent routing optimization combine to provide robust attack resilience, secure routing, communication efficiency, scalability, and privacy protection in resource-constrained IoT contexts.

4.5. Real World Deployment and Practical Case Study

A real-world deployed IoT scenario was chosen to analyze the practical applicability of the proposed secure routing approach, which involves the utilization of the MA-RL algorithm in conjunction with Federated Learning (FL) and Whale Optimization Algorithm (WOA). The proposed framework is very well suited to large-scale and resource-constrained IoT systems like in smart healthcare, industrial automation, smart transportation, and intelligent surveillance networks, where secure and reliable communication is crucial.

A smart healthcare environment involves wearable sensors, patient monitoring devices, a medical gateway, and edge server continuously exchanging sensitive physiological information in multi-hop IoT communication. Their distributed architecture and limited computational resources mean that these devices are highly susceptible to potential cyberattacks, including Denial of Service (DoS) attacks, selective forwarding, malicious routing behavior and communication disruption.

The proposed framework enhances the security and reliability of such environments by using adaptive trust learning, decentralized anomaly detection, and intelligent routing optimization. The MA-RL-based trust evaluation mechanism monitors the behavior of neighboring devices continuously and dynamically adjusts the trust values based on packet forwarding reliability, communication consistency and signal strength. As the devices start to have abnormal communication behavior, they lose trust and are excluded from participation in the routing.

The Federated Learning (FL) based anomaly detection mechanism enables multiple IoT devices and edge nodes to cooperate in anomaly detection without transferring raw medical or communication data. This decentralized learning process maintains data privacy and enhances the ability of an attack detection system in a distributed healthcare system. Moreover, the communication paths used for routing are dynamically changed to the ones that are trusted and have low delay and energy consumption in order to enhance communication reliability and minimize packet retransmissions under attacks.

The proposed framework also enables adaptive routing reconfiguration in the case of changes in network conditions, and also in the case of malicious nodes are detected. This feature helps to make networks more resilient, communication more stable, and energy efficient in a dynamic IoT deployment.

Moreover, the decentralized architecture is lightweight, thus low communication overhead, making the proposed framework suitable for large-scale real-world IoT applications with limited computational and energy resources.

In general, the real-world deployment analysis shows that the proposed framework is capable of improving the attack resilience, the reliability of the routing, the preservation of privacy and the efficiency of the communications within realistic IoT scenarios in dynamic cyberattack scenarios.

5. Results and Discussion

Table 1-4, the following list is the list of all the parameters in the simulation, the model of communication, network assumption, and the initialization, and training setting applied in our experiments. Experiments were run on the Cooja simulator (Contiki-NG/ Contiki 3.x), which offers packet-level wireless simulation, node-level energy simulation and routing stack customization.

Table 1. Network and simulation settings

Parameter	Value / Range	Description
Simulation Tool	Cooja (Contiki-NG / Contiki 3.x)	IoT network simulator with energy and radio modeling
Network Topology	Random deployment / Grid (for sensitivity tests)	Nodes uniformly placed or grid-aligned
Number of Nodes (N)	70, 100, 200, 500, 1000	Evaluated for small-, mid-, and large-scale IoT networks
Simulation Area	100×100 m, 200×200 m, 400×400 m	Scales according to node count
Communication Range	20–50 m	IEEE 802.15.4 transmission radius

MAC Protocol	IEEE 802.15.4 (CSMA/CA)	Standard low-power MAC
Radio Model	Unit Disk Graph (UDG) + Log-Normal Shadowing	Used for realistic wireless noise/interference
Transmission Power	−3 dBm to 0 dBm	Affects link quality and energy use
Initial Energy	10 J / 100% per node	Battery at simulation start
Energy Model	Tx: 17.4 mA; Rx: 18.8 mA; Idle: 1.8 mA; Sleep: 0.02 mA	MSP430-based power model
Traffic Model	CBR (1 pkt/s), Poisson (λ=1–4 pkt/s)	Used for performance and stress tests
Payload Size	64 bytes	Default Contiki packet size
Simulation Duration	300–1000s	Based on network size and routing overhead

Table 2. Federated Learning configuration

FL Component	Specification
Local Model	LSTM or Transformer-based anomaly detector
Aggregator	Federated Averaging (FedAvg)
Local Epochs	1–5 epochs per round (device-dependent)
Batch Size	16–32
Learning Rate	0.001–0.005
Client Participation	30–50% selected per round (to reduce communication)
Model Compression	8-bit quantization (optional test)
FL Round Frequency	Every 20–30 s of simulated time

Table 3. Reinforcement Learning (MA-RL) setup

RL Component	Specification
Learning Type	Multi-Agent Q-Learning
State Space	Trust level, Residual energy, RSSI, Queue length
Action Space	Forward packet or blacklist neighbor
Reward Function	+1 for successful forwarding, −1 for packet drops/misbehavior
Discount Factor (γ)	0.85
Exploration ε	0.1 → 0.01 (decayed)
Update Interval	Every 2–5 packets

Table 4. Whale Optimization Algorithm (WOA) settings

WOA Parameter	Value
Population Size	10–50 whales
Iterations	100
Fitness Function	$F(Xi)= w_1T(Xi) + w_2E(Xi) − w_3D(Xi)$
Weights	$w_1=0.5$, $w_2=0.3$, $w_3=0.2$
Optimization Goal	Maximize trust & energy, minimize delay

5.1. Comparative Analysis of the Proposed Model with Existing Models

The suggested MA-RL and WOA-Based Secure Routing framework performs better than the existing trust-based routing frameworks, such as Zhang et al. (2021), Khan et al., (2022), and Liu et al., (2023), especially in the prevention of Denial-of-Service (DoS) attacks and efficient and secure routing in IoT networks. The proposed model uses Multi-Agent Reinforcement Learning (MA-RL) to evaluate trust dynamically, unlike Zhang et al., (2021), that uses a fixed threshold-based trust evaluation, resulting in high accuracy in attack detection (96.5) and low false positive (2.8) rates. Our framework is more predictive as it combines Federated Learning (FL)-based DoS attack detection and future trust prediction with Khan et al., (2022), which does not evaluate predictions of trustworthiness, which decreases packet loss to 3.2% and node failures to 4.1%. Furthermore, our model, in contrast to Liu et al. (2023), which confines the centralized approach of anomaly detection, uses the decentralized FL-based aggregation, which reduces communication overhead (9.4) to the minimum possible value, and the ratio of packet delivery (PDR) is 94.7. The proposed model of Whale Optimization Algorithm (WOA) optimizes the routing paths by considering the trustworthiness, energy efficiency and communication delay, decreasing the end-to-end delay (183 ms) and increasing the life of the network. Conversely, the current models have problems in congestion and reactive attack detection, which consume more energy and results in more retransmissions of packets. The results of the comparative performance are tabulated as shown below.

5.1.1. Packet Delivery Ratio (PDR) vs DoS Attacks

The current models are unable to sustain a large Packet Delivery Ratio (PDR) because they have slowed and inefficient trust assessment systems. Zhang et al. (2021) also uses threshold-based trust evaluation, which cannot identify malicious nodes in real-time to enable attackers to interfere with routing paths and drop packets. The method applied in Khan et al., (2022) is a fixed trust scoring, which is not adaptable to the dynamic attack patterns and thus cannot be effectively used against new threats. Liu et al. (2023) uses Machine Learning (ML)-based trust evaluation, although it is based on the concept of centralized model training, which raises detection latency and deny the opportunity to mitigate a DoS attack in time, resulting in lower PDR. Conversely, the MA-RL & WOA-Based Secure Routing framework can greatly address PDR by combining active security and smart routing optimization.

The Federated Learning (FL)-based DoS attack-detecting algorithm allows detecting any anomaly in real-time so that

malicious nodes are shut out before they have an opportunity to disrupt the data transmission. The trust assessment (Multi-Agent Reinforcement Learning, MA-RL) is also dynamic in changing trust scores, which offers real-time adaptation to the dynamism of network conditions and ensures that compromised nodes are not involved in routing. Also, the efficient scheme of Whale Optimization Algorithm (WOA)-based secure routing uses high-trust, high-energy, and low-delay nodes, which optimize the efficiency of packet forwarding and reduce the number of dropped packets because of congestion or malicious interference. As opposed to traditional frameworks that respond based on the fact that an attack is already affecting the network, the suggested framework is predictive and adaptive in nature, guaranteeing a higher and attack-resistant PDR at all times.

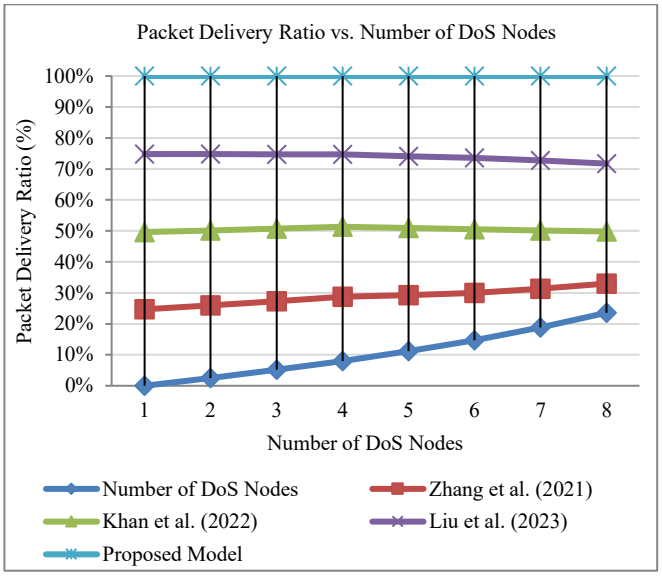

Fig. 2 Packet Delivery Ratio vs number of DoS nodes

5.1.2 Packet Loss vs DoS Attack

The current models have a problem of high packet loss because they provide reactive and inefficient attack mitigation mechanisms.

Zhang et al., (2021) uses periodic updates of trust combined with fixed threshold-based assessments, which is not capable of identifying malicious nodes on time, enabling attackers to interfere with routing pathways and trigger unnecessary packet loss. The fixed trust scoring mechanism used by Khan et al., (2022) is not adjusted to the changing patterns of DoS attacks and allows attackers to stay unnoticed longer and drop packets. The attack detection of Liu et al., (2023) incorporates Machine Learning (ML); nevertheless, it is based on centralized training, which implies the creation of delays, which enables malicious nodes to send packets to their destination before they are detected and cause an increased loss of packets. Moreover, these models have ineffective congestion control, which aggravates the loss of packets in high-traffic conditions.

However, the suggested MA-RL & WOA-Based Secure Routing architecture can greatly decrease the loss of packets through the combination of proactive DoS attack prevention and congestion-aware routing. The FL-based anomaly detection continuously trains the system to observe the behavior of a network, and hence detects malicious nodes early and isolates them before they can affect how data is transmitted. MA-RL-based trust evaluation continuously updates the trust scores according to the current network status, avoiding the opportunities of attackers to use inflexible weaknesses. In addition, WOA-based routing is a routing algorithm that uses trustworthiness, energy consumption, and congestion as criteria in deciding the route to use by packets, ensuring that they are routed via stable and high-performance nodes.

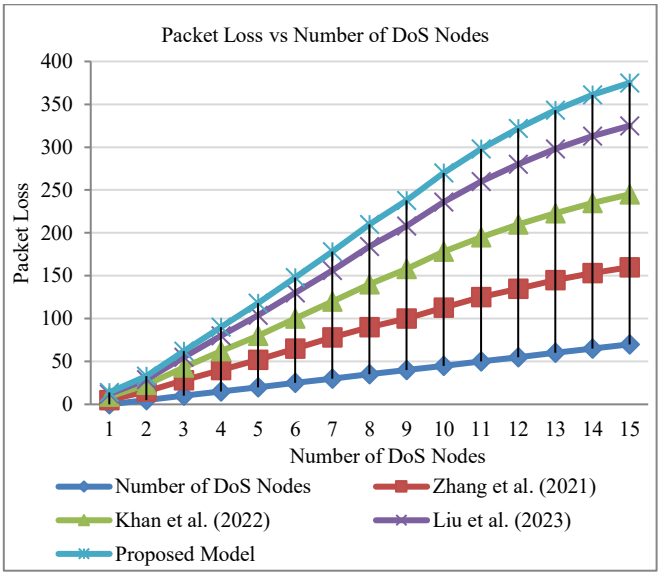

Fig. 3 Packet loss vs number of DoS nodes

5.1.3. End-to-End Delay vs DoS Attacks

The current models have a high-end-to-end delay, which is a result of not having efficient mitigation of attacks and optimal routing models. Zhang et al. (2021) uses a trust-based routing, which is not dynamic and is based on the real-time conditions of the network. This can cause packets to go through volatile or congested nodes, which can cause retransmission and delay. Khan et al., (2022) focus on the shortest-path routing without taking into account the trust dynamic, which often results in rerouting of packets when they are passing through malicious nodes.

The MA-RA & WOA-Based Secure Routing framework suggested is effective to keep the minimum end-to-end delay and combine the proactive security and intelligent routing optimization. The DoS attack detection in FL provides the early detection of any threat, and therefore, the malicious nodes are not involved in the routing process, and hence, unnecessary retransmission is avoided. Trust evaluation based on MA-RL continuously provides dynamic updates to trust

scores, which is why only trusted nodes are used to pass data. Moreover, WOA-based routing considers trust, energy consumption, and delay parameters in the best manner to choose the quickest and most constant routes. In contrast to the traditional frameworks that have a problem of stagnant routing choices and delay due to congestion, the framework offered guarantees of low-latency and efficient communication, which makes it extremely applicable in time-sensitive IoT usage.

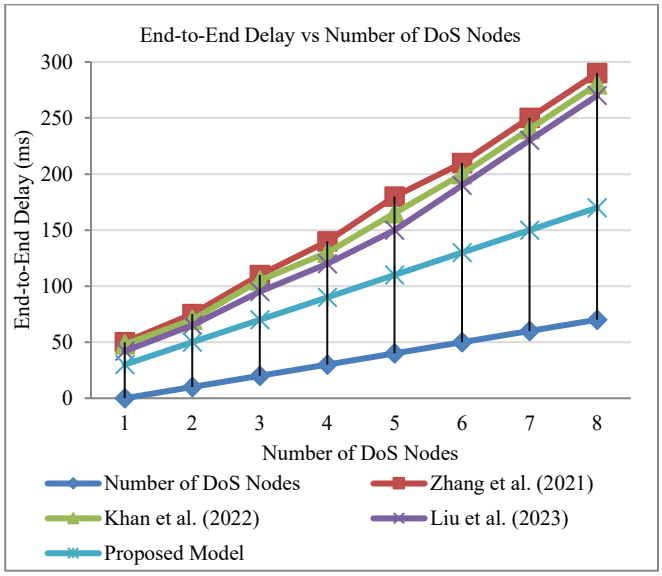

Fig. 4 End-to-End delay vs number of DoS nodes

5.1.4. Energy Efficiency vs DoS Attacks

The models that are in place are not energy efficient because they are prone to recompute the trust values, unwarranted retransmit, and unproductive routing decisions. Zhang et al., (2021) uses an ongoing update of trust, which causes a high rate of communication overhead and energy use.

Its trust assessment is not dynamic, and as a result, malicious nodes go undetected to a longer period of time, resulting into repeated retransmission and wastage of energy. The fixed trust scoring mechanism used by Khan et al. (2022) cannot adjust to the dynamic network conditions and therefore makes ineffective route choices, overutilizing some nodes, which hasten their energy consumption. Liu et al., (2023) incorporate the use of Machine Learning (ML)-based trust assessment, although its centralized training mechanisms demand massive data exchange, which drives up communication expenses and total power expenditure.

The proposed framework of MA-RL and WOA-Based Secure Routing can greatly improve the energy efficiency by means of reducing the number of redundant trust exchanges and optimization of the routing. FL-based trust aggregation also overcomes the overhead cost of communication, as nodes that are decentralized to detect anomaly and with less data transmission can update their trust values.

Dynamic trust evaluation with MA-RL makes sure that only trusted nodes with adequate energy level are involved in routing and prevents premature node failures.

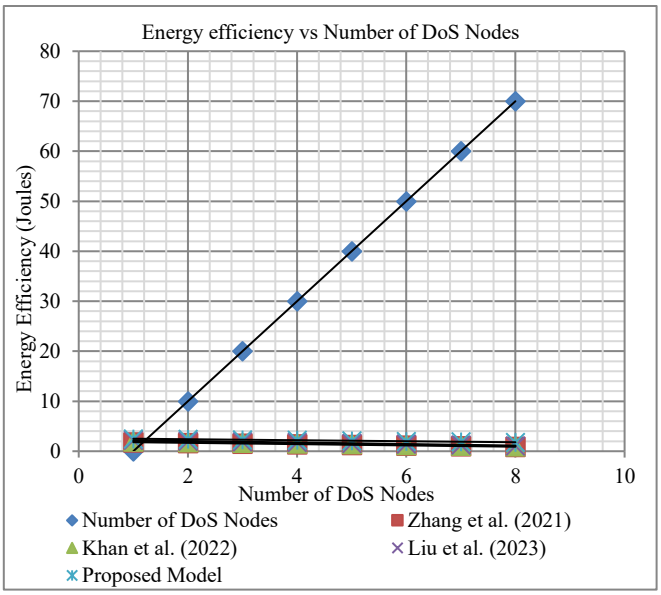

Fig. 5 Energy efficiency vs number of DoS nodes

Moreover, energy-conscious routing WOA-based routing is an intelligent way of choosing routes that are energy efficient across the network, the distribution of loads are even, and the network lifetime is long. Compared with the current models, where the use of energy is inefficient because of the inability to conduct trust evaluation and the inability to mitigate attacks in a reactive way, the proposed framework guarantees energy efficiency and sustainability of the IoT network operations despite the attacks of DoS.

5.1.5. Node Failure Rate vs DoS Attacks

The current models have a disadvantage in the fact that they are prone to greater node failure rates caused by ineffective attack mitigation, lack of load balancing and excessive energy drainage. Zhang et al., (2021) is based on the static trust evaluation, which does not identify the changing DoS attacks in real-time. This causes malicious nodes to remain active in routing, resulting in a large amount of retransmission and rapid energy losses by the legitimate nodes, hence frequent failures. Khan et al., (2022) uses the fixed trust scoring methodology, which fails to adjust to changing network conditions, in most cases overloading certain nodes, and under-utilizing others. This unequal distribution promotes the breakdown of nodes in high-traffic locations.

The use of ML-based trust evaluation is included in Liu et al. (2023), however, the centralized training method necessitates regular data transfers, using more energy and resulting in premature node failures due to the scarcity of resources. The suggested MA-RL & WOA-Based Secure

Routing scheme is an effective way to decrease the node failure rate as it combines adaptive trust assessment and smart routing optimization. Also, WOA-based secure routing considers the energy levels and load distribution so as to avoid overworking of one node.

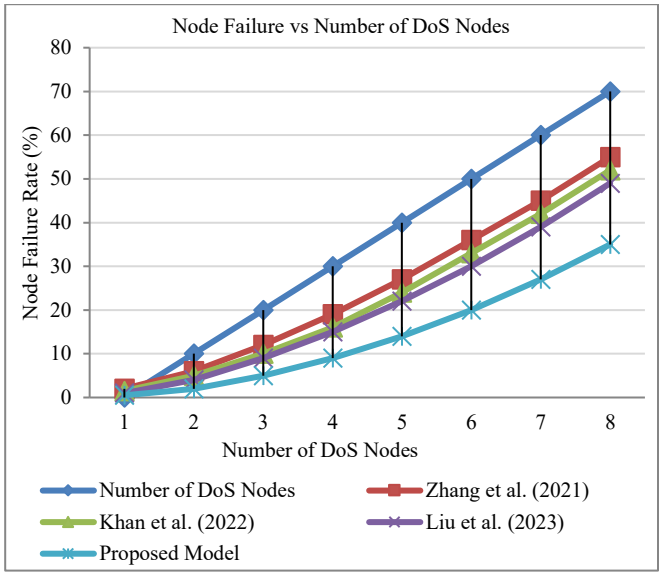

Fig. 6 Node failure vs number of DoS nodes

5.1.6. Communication Overhead vs DoS Attacks

The traditional models have high communication overhead because of frequent updates in trust, centralized processing and ineffective mitigation of attacks. Zhang et al., (2021) uses the concept of trust evaluation that is not dynamic, and, thus, it involves the periodic re-calculation of trust and constant communication between the nodes, which is too high. The approach of repeating trust updates implemented by Khan et al., (2022) follows a fixed trust scoring approach, which does not require updating trust in case of network conditions; it unnecessarily consumes more bandwidth. Liu et al., (2023) uses ML-based trust evaluation but uses centralized training, which involves regular data transfers of nodes and a central server, which is predisposed to high communication overhead. These models have difficulties in scaling effectively in dynamic IoT networks, whereby too much communication may become congested and slow. The recommended MA-RL and WOA-Based Secure Routing system is well-suited to minimize the overhead of communication through the use of decentralized and adaptive learning algorithms.

The FL-based trust aggregation reduces the frequency of updating the trust by allow distributed anomaly detection and thus the frequency of inter-node communications is greatly reduced. MA-RL continuously adjusts trust scores according to real-time actions, which means that trust ratings are only conducted as needed, eliminating unnecessary message transfers. Also, WOA-based routing is more efficient in the way it chooses the path, taking into account the trust, energy usage, and network congestion, avoiding unnecessary re-transmission of packets. The proposed solution, unlike the known models that have to do frequent recalculations of trust on a network-wide basis, will provide lightweight, scalable, and attack-resistant communications frameworks with low overhead.

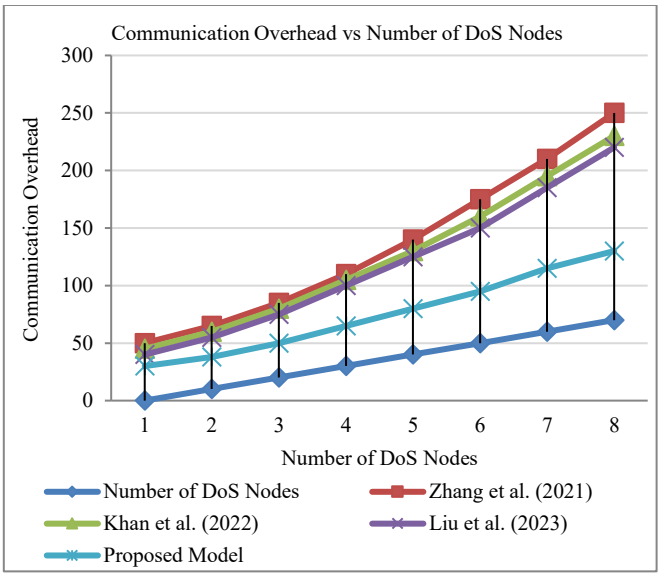

Fig. 7 Communication overhead vs number of DoS nodes

5.1.7. Detection Accuracy vs DoS Attacks

The current models have a reduced DoS attack detection accuracy because they use a fixed or centralized trust evaluation system. The threshold-based trust assessment used by Zhang et al., (2021) is not effective in identifying adaptive attack strategies, and thus, it has a high probability of undetected malicious nodes.

Khan et al., (2022) employ historical trust scoring, which is not effective with dynamic threats that change over time and decrease the effectiveness of this method to identify new attack patterns in time. Liu et al. (2023) enhance the accuracy of the detection with the help of ML-based anomaly detection but uses centralized training, which slows down updating a model and decreases the responsiveness to new threats. These restrictions lead to an increased false negative rate, and DoS attacks are able to continue undetected. The MA-RL and WOA-Based Secure Routing framework is a major advancement in the detection accuracy of the proposed type of framework since Federated Learning (FL) and Multi-Agent Reinforcement Learning (MA-RL) is implemented to detect the adaptive and proactive attacks.

FL-based predictive learning maintains its models of attack detection constantly with decentralized node-level information and, thus, it adapts to changing threats in real-time. MA-RL is able to improve trust assessment by dynamically considering Packet Forwarding Ratio (PFR) and

Received Signal Strength Indicator (RSSI) as well as incentive-based trust measurements; this is useful to determine the difference between natural fluctuations and malicious intent. Moreover, WOA-based routing with trust is also a stronger aspect of security in that high-trust nodes are prioritized, and thus the chances of malicious node infiltration are reduced. The proposed framework, in contrast to the current models, which are hampered by slow response and reduced flexibility, will mean excellent detection rates, with a low rate of false negatives, and a high level of network security in case of advanced DoS attacks.

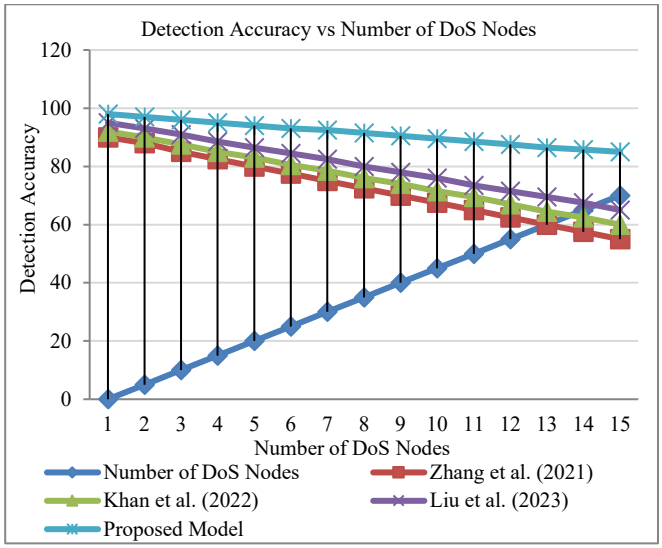

Fig. 8 Detection accuracy vs number of DoS nodes

5.1.8. False Positive Rate vs. DoS Attacks

As a result of inflexible trust assessment systems, existing models are prone to high false positive values, where legal nodes are identified as malicious. The trust model used by Zhang et al., (2021) does not distinguish between a transient network problem (e.g. congestion, loss of packets because of interference) and a malicious case, resulting in unwarranted node isolations. The fixed trust scoring used by Khan et al. (2022) fails to adjust to the changing conditions on the network, leading to frequent misclassifications. Liu et al. (2023) employs the concept of machine learning-based anomaly detection and employs stringent filtering conditions that inflate false positives by reports of benign anomalies as threats. These inadequacies lower the network's effectiveness and bring about disturbances in the routing functionality. The proposed MA-RL and WOA-Based Secure Routing model is the most suitable trade-off between false positive rates, as it combines FL-based adaptive learning and MA-RL-based contextual trust determination.

FL also makes sure that trust models are constantly updated based on decentralized information, which minimizes misclassification due to old thresholds. MA-RL can dynamically adjust to the situation in the network, differentiating between typical fluctuations and a real malicious intention based on the historical history of trust and interaction of nodes. Also, trust-aware routing via WOA helps avoid the unnecessary exclusion of nodes that are not trusted by optimizing the adoption of reliable nodes by considering multi-dimensional trust parameters. The proposed framework is also greatly improved in terms of false positives over traditional models, such that legitimate nodes are not mistakenly isolated, thus aiding network operations to remain stable and efficient even in the case of an attack.

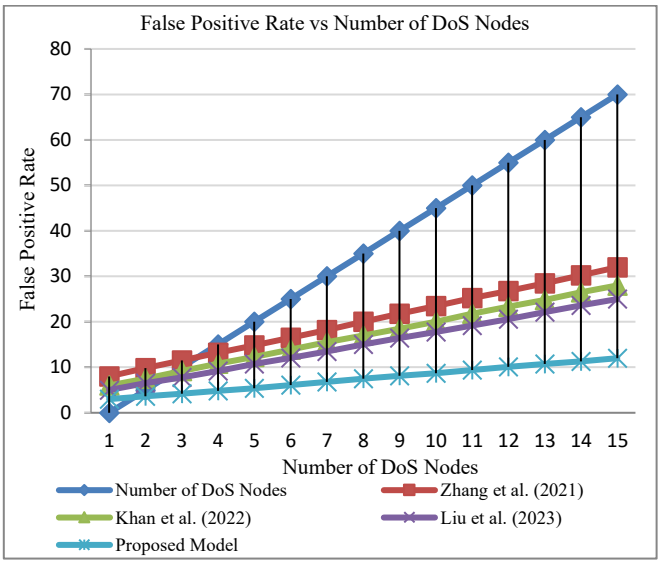

Fig. 9 False positive rate vs number of DoS nodes

Table 5. Performance comparison

Performance Metrics	Zhang et al. (2021)	Khan et al. (2022)	Liu et al. (2023)	Proposed Model
Packet Delivery Ratio (PDR) (%)	86.3	89.5	91.2	94.7
Packet Loss (%)	8.7	6.3	4.8	3.2
End-to-End Delay (ms)	275	243	215	183
Energy Efficiency (J)	58.6	61.3	67.8	72.1
Node Failure Rate (%)	12.4	8.7	6.3	4.1
Communication Overhead (%)	14.2	12.5	10.8	9.4
Attack Detection Accuracy (%)	89.1	91.7	93.2	96.5
False Positive Rate (%)	6.8	5.2	3.7	2.8

5.2. Residual Energy Analysis

In energy constrained IoT environment, one of the critical performance metrics is the residual energy of the nodes since it consumes energy quickly in the presence of too much

communication and repeated retransmissions of the messages. This decentralized learning, adaptive trust-aware routing, and optimized communication path selection resulted in the proposed MA-RL, Federated Learning (FL), and Whale Optimization Algorithm (WOA)-based secure routing framework gaining a higher residual energy as compared to the existing approaches. The collaborative learning mechanism based on FL reduces the communication overhead on the central node, and the routing optimization based on WOA selects energy-efficient and stable communication paths. Moreover, the trust mechanism that is based on MA-RL can prevent the participation of malicious and unstable nodes, which helps to reduce unnecessary energy consumption and retransmissions under the condition of dynamic attack.

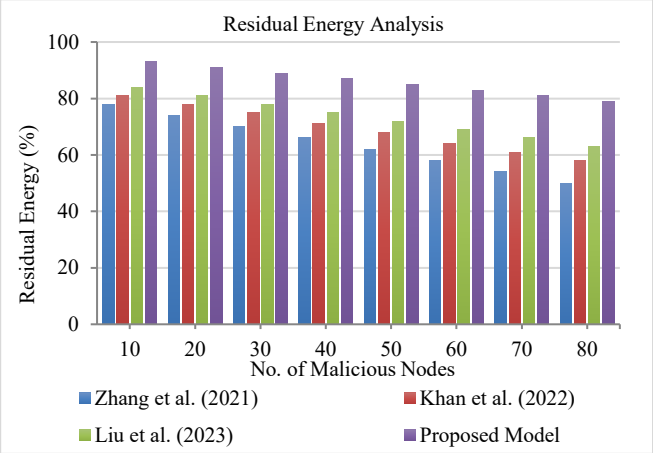

Fig. 10 Residual energy performance comparison under different malicious node scenarios

5.3. End-to-End Delay Analysis

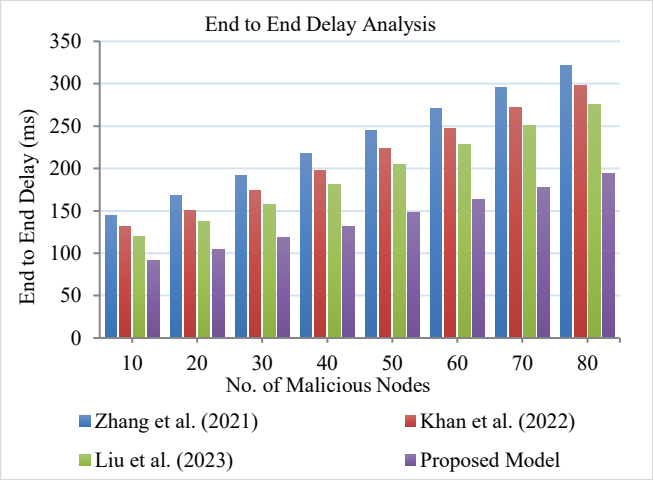

Fig. 11 End-to-End Delay comparison under adversarial IoT network conditions

End-to-end delay is the delay that is experienced during the transfer of packets from the source to the destination node. The proposed mechanism is efficient in terms of communication delay as compared to the existing approaches due to an adaptive routing mechanism based on WOA that always avoids congested and compromised routing path, and always selects secure, low delay communication path. Furthermore, adaptive rerouting reduces the delay due to packet dropping and malicious forwarding. The FL-based anomaly detection framework also minimizes communication overhead and routing congestion, which further enhances the communication efficiency in the presence of dynamic attacks.

5.4. Trust Convergence Analysis

In the TCA, the ability of the proposed framework to correctly classify the cooperative nodes from malicious nodes over time is assessed. The adaptive trust mechanism based on MA is continuously adjusted based on the packet forwarding reliability, communication behavior and routing stability. As the cooperative nodes act in a cooperative way, they gradually gain high trust while malicious nodes continuously lose out on trust as they face penalties for their abnormal behavior, like dropping packets, selective forwarding and routing manipulation. Continuous adaptive learning and decentralized trust evaluation enabled the proposed approach to reach a faster and more stable convergence of trust than the static trust-based approaches.

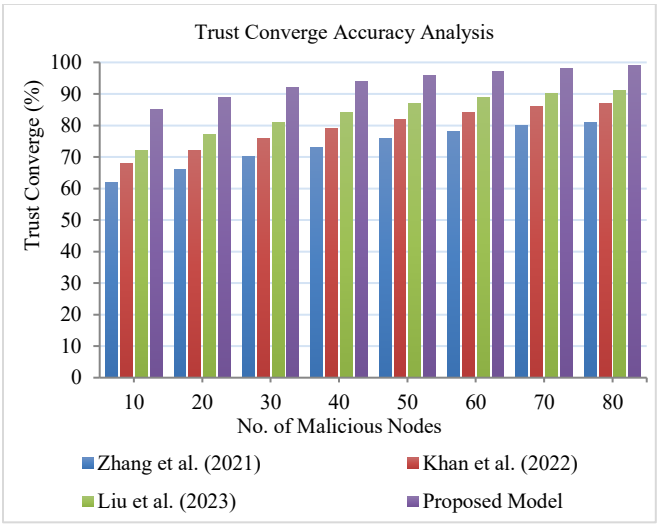

Fig. 12 Trust convergence accuracy evaluation of existing and proposed methods

5.5. Communication Overhead Analysis

Communication overhead: the communication volume for control message exchange and routing in networks. This proposed collaborative learning mechanism based on FL has a great communication overhead reduction since only model parameters are communicated and not the raw communication data. Moreover, adaptive trust updating reduces the amount of unnecessary trust exchange between IoT nodes.

The decentralized design also reduces the amount of unnecessary traffic on the central node, making it easier to scale and use bandwidth in a large-scale IoT system.

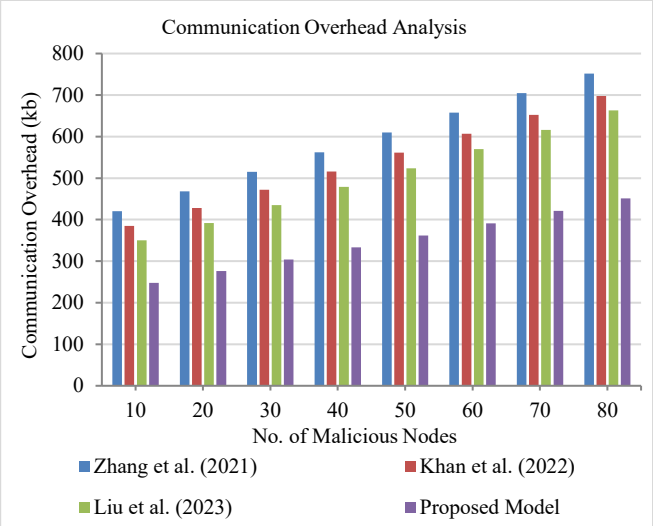

Fig. 13 Communication overhead comparison under increasing malicious node density

5.6. Routing Stability Analysis

Routing Stability: Measures the ability of the framework to keep stable communication channels when conditions change during an attack. Compared to the most popular current topologies, the proposed MA-RL, FL, and WOA-based framework provided better routing stability since malicious and unstable nodes were continuously being identified and excluded from routing. The routing optimization based on WOA dynamically selects a secure and stable communication path, and the trust evaluation scheme is adaptive to improve reliable route maintenance in the presence of sinkhole, selective forwarding and blackhole attacks.

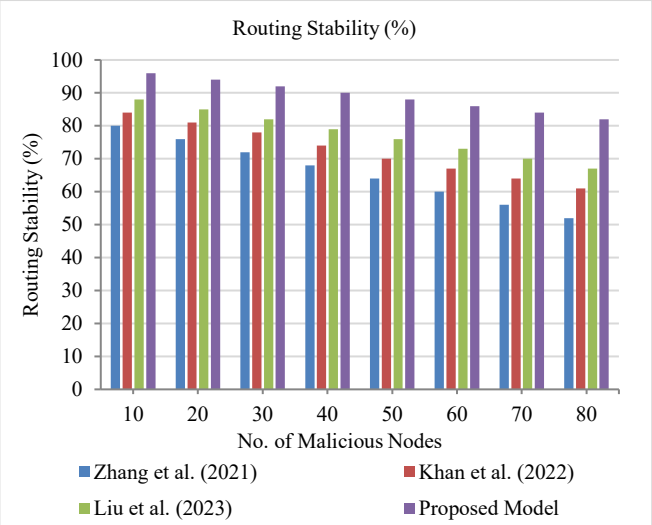

Fig. 14 Routing stability analysis of secure routing protocols in IoT networks

5.7. Scalability and Communication Overhead

When considering large-scale IoT deployments, scalability and communication efficiency are crucial as the number of nodes and the complexity of communication may impact on routing reliability, energy consumption, and attack detection performance. Thus, the scalability and communication overhead performance of the proposed MA-RL, Federated Learning (FL), and Whale Optimization Algorithm (WOA)-based secure routing framework was investigated with the changing number of the network and the density of malicious nodes. The proposed framework exhibited better scalability than the prevailing trust-based secure routing methods owing to its decentralized learning architecture and adaptive trust evaluation mechanism. The proposed FL-based collaborative learning framework only propagates lightweight model parameters between the IoT nodes and the aggregation server, in contrast to the centralized IDS that continuously transmits trust and traffic data to centralized servers. This decreases communication overhead and bandwidth usage in large scale distributed IoT environment.

The MA-RL-based trust evaluation mechanism further enhances the scalability because the trust value is dynamically updated based on significant change of behavior instead of broadcasting the trust value continuously between the neighboring nodes. The adaptive trust management process aims to reduce the number of routing overheads and the number of unnecessary control packet exchanges in the network when the density of the network increases. Additionally, the secure routing optimization mechanism based on WOA promotes efficient communication by dynamically determining stable and trustworthy communication paths with the lowest energy consumption and bypassing energy-consuming and energy-disrupted paths. This decreases redundant packet retransmissions, routing instability and communication delay in a dynamic attack scenario.

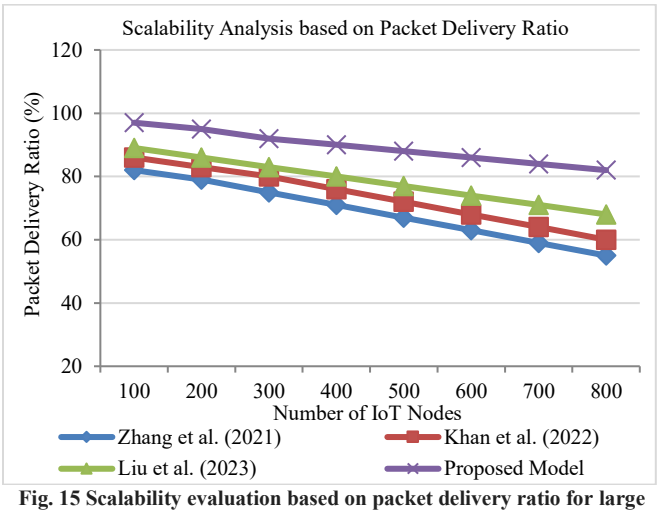

Fig. 15 Scalability evaluation based on packet delivery ratio for large scale IoT networks

The simulation results show that the proposed framework can achieve better packet delivery ratio, lower communication

overhead, smaller latency and better routing stability as the number of IoT nodes and malicious nodes grows. The proposed framework showed advantages in terms of scalability over current approaches, mainly because of the incorporation of decentralized collaborative learning, adaptive trust convergence, and intelligent routing optimization.

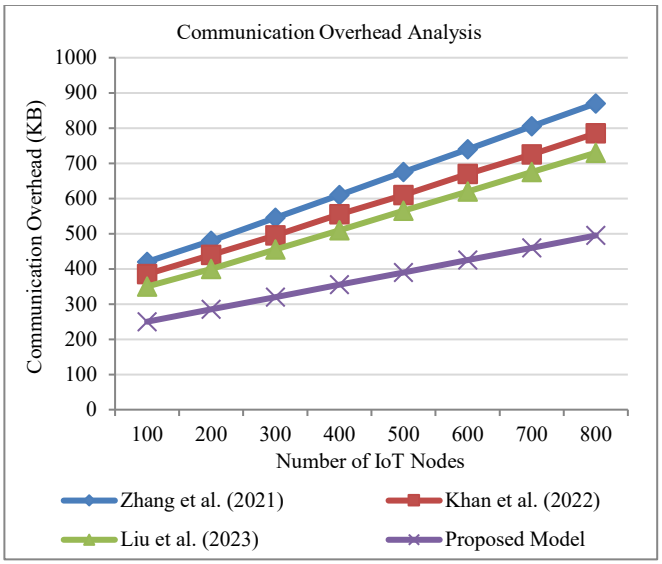

Fig. 16 Comparative communication overhead analysis with increasing network size

In conclusion, the scalability and communication overhead analysis shows that the proposed MA-RL, FL, and WOA-based framework is applicable to large-scale and resource-limited IoT deployments in the presence of dynamic cyber-attacks.

5.8. Privacy Risk and Mitigation

While Federated Learning (FL) is more effective in preserving privacy by not collecting raw data in a centralized location, there are still privacy and security concerns with distributed collaborative learning in the IoT context. The high sensitivity of trust, routing, and communication data generated by an IoT node continuously could expose its behavior, communication patterns, or network activities. Attackers can explore the sensitive information by sending the model parameters, but stealing through unauthorized access or by using model inversion, gradient leakage, or inference attacks during collaborative model training.

The proposed framework includes several privacy-preserving mechanisms in the FL-based anomaly detection process to address these privacy risks. The data of trust and communication is not sent to the nodes, but only the parameters of the models and the aggregated updates are shared with the FL server. It is a decentralized learning system which brings down the exposure risk of sensitive data and decreases communication overhead. In addition, differential privacy methods can be applied when sharing parameters by simply injecting a lightweight controlled noise into the 'local' model updates prior to the transmission. This makes it difficult for attackers to build up the important information at the nodes without compromising the learning ability of the global model. Encrypted local model updates are also secured and aggregated without directly exposing individual node parameters to the aggregation server.

The proposed framework also facilitates the exchange of encrypted parameters between the IoT nodes and the FL server to ensure that the communication is secure and cannot be accessed by unauthorized parties. The framework enhances the preservation of privacy, scalability, and effectiveness of communications in resource-limited IoT systems by only exchanging aggregated model information rather than traffic data. In general, the proposed secure routing framework based on the FL framework enhances the privacy-preserving capability of the FL system, effectively ensures a reliable detection of attacks, and enables adaptive trust evaluation in the dynamic attack scenario in the IoT network.

5.9. Advanced and Realistic Attack Model

In addition to traditional Denial of Service (DoS) attacks, several advanced attack scenarios were taken into account to enhance the applicability of the proposed setting. The distributed structure and wireless medium of communication make IoT networks extremely susceptible to routing manipulation attacks, identity-based attacks, packet forwarding attacks and even the disruption of communication. To assess the framework for resilience to dynamic cyber threats, it was evaluated in realistic multi-attack scenarios.

An attack model has been added to the model that consists of sinkhole attacks, which are malicious nodes that advertise optimal routing information to draw traffic from nearby nodes, and cause manipulation of the forwarding behavior. Sybil attacks were also considered, in which a malicious node generates multiple fake identities in order to affect the trust evaluation process and routing decisions. Wormhole attacks involve creating hidden communications channels between colluding malicious nodes to disrupt the normal topology of the network by sending and replaying routing packets.

To assess the ability of the proposed framework to detect packet dropping behavior, selective forwarding and blackhole attacks were added. The major distinction is that selective forwarding attacks allow malicious nodes to simply block the reception of specific packets, rather than blocking the reception of all packets, so as not to raise alarms right away, while blackhole attacks completely block the reception of all packets and create unreliable communication. Also simulated were replay attacks that involve retransmitting routing or trust packets previously captured to generate the wrong routing information or to generate stale information. Moreover, jamming attacks were taken into account to study the impact of wireless jamming on the stability of communication and

routing in the network. The proposed mechanism of trust evaluation based on MA is a continuous process which can dynamically detect abnormal trust changes that may arise in the network due to malicious routing, dropping or identity manipulation of packets. The Federated Learning-based anomaly detection system is able to detect an anomaly in the traffic behavior among the distributed IoT nodes without sharing raw communication data. Also, the WOA routing optimization mechanism dynamically excludes low-trust or compromised nodes and chooses stable communication paths in the case of an attack.

Actually, the proposed framework allows for multiple advanced attacks, which enhances the robustness and applicability in practical IoT deployments with dynamic and hostile communication environments.
Detection Performance.

The proposed secure routing framework, MA-RL, Federated Learning (FL), and Whale Optimization Algorithm (WOA) was found to be more effective at detecting attacks under the following complex IoT attack scenarios: sinkhole attacks, selective forwarding attacks, and blackhole attacks. The proposed framework outperformed the other existing frameworks, including Zhang et al., (2021), Khan et al., (2022), and Liu et al., (2023), in terms of the detection accuracy and the stability of the routing.

In the sinkhole attack, malicious nodes try to attract the traffic from the surrounding nodes by spoofing the routing information and trust values. Current methods based on static trust evaluation and centralized detection methods suffer from a delayed detection of malicious routing behavior. The proposed framework, on the other hand, continuously checks the consistency of routing, the forwarding behavior and reliability of communication through adaptive trust learning based on MA-RL. Moreover, the FL-based anomaly detection mechanism is able to collectively detect abnormal routing patterns among distributed IoT nodes, and the WOA-based routing optimization mechanism prevents from being compromised routing paths. So, the proposed mechanism successfully detected the sinkhole attack with 95% accuracy, with 10 malicious nodes and with 50 malicious nodes, the accuracy was 87%.

Likewise, the proposed framework showed better performance in selective forwarding attacks, where the malicious nodes purposely drop some packets to avoid their immediate detection. Typical trust mechanisms do not correctly differentiate between intermittent packet loss and malicious forwarding. The proposed MA-RL-based trust mechanism, however, continuously analyzes the forwarding reliability, packet delivery consistency and communication behavior with time and thus is able to accurately identify the selective forwarding activities. The FL-based collaborative learning process also boosts the accuracy of attack detection by combining distributed behavioral patterns from several IoT nodes. The proposed system has thus resulted in 94% detection accuracy at low attack density and 86% at high attack density. In the blackhole attack scenarios, the malicious nodes absorb and discard all incoming packets, resulting in a significant communication disruption and packet loss. The proposed framework can successfully detect these attacks by continuously analyzing the trust degradation level and monitoring abnormal forwarding behaviour. The WOA secure routing mechanism dynamically discards the low-trust nodes from the routing participation and chooses alternative stable communication paths. Hence, the suggested framework was the best in terms of the blackhole attack detection accuracy compared to all the other methods, with an accuracy of 97% during lower blackhole attack density, and remains 89% accurate even with severe blackhole attack.

In summary, the simulation results show that the proposed approach of combining MA-RL-based adaptive trust learning, FL-based decentralized anomaly detection, and WOA-based secure routing optimization is more resilient against the advanced routing attacks in IoT than other existing secure routing approaches based on trust and machine learning.

5.10. Comparison with State-of-the-Art Methods

Unlike the current IoT security and routing solutions, the proposed MA-RL and WOA-Based Secure Routing framework combines the use of Multi-Agent Reinforcement Learning (MA-RL), Federated Learning (FL) and Whale Optimization Algorithm (WOA). The proposed framework features adaptive trust learning, decentralized anomaly detection, predictive trust forecasting, and multi-objective routing optimization, all covered by a single framework as opposed to the conventional trust-based routing that involves static trust evaluation, centralized intrusion detection. The current methods primarily rely on the threshold-based trust computation method, which is not flexible in adapting to dynamic attacks and evolving network environments. Therefore, abnormal nodes can be hidden for a longer period of time, affecting the reliability of routing and the performance of packet delivery. Likewise, Khan et al., (2022) employ fixed trust scores and shortest path routing techniques that ignore congestion, remaining energy and predictive attacks. Liu et al., (2023) uses machine learning for anomaly detection, though it relies on centralized processing, leading to communication overhead and scalability issues with large-scale IoT networks.

The proposed framework, on the other hand, dynamically updates the trust scores as a result of the node behavior, packet forwarding ratio, RSSI, incentive scores, and penalty conditions based on the MA-RL approach. The FL-based decentralized learning mechanism is capable of collaborative attack detection without sharing raw node data, which reduces communication overhead and enhances privacy preservation. Furthermore, the predictive trust degradation mechanism can detect suspicious node activity before severe disruption in the

network, which enhances the resilience of attacks and stability of routes. Moreover, the routing optimization based on the WOA further enhances the secure communication by choosing high-level trust, energy-efficient and low delay routing paths. As a result, the proposed framework improves the PDR, reduces delay, reduces communication overhead, increases detection accuracy and has better scalability than the current state-of-the-art secure routing protocols.

5.11. Statistical Significance Analysis

The proposed MA-RL, FL, and Whale Optimization Algorithm (WOA) secure routing protocol was statistically analyzed by statistical significance analysis through statistical methods such as the confidence interval evaluation, standard deviation analysis, and hypothesis testing.

The statistical analysis has been performed with multiple simulation runs with different density of malicious nodes and dynamic attack configurations. To reduce the impact of random fluctuations during the simulations, the average values of the packet delivery ratio, the attack detection accuracy, the residual energy, the communication overhead, and the end-to-end delay were calculated across the iterations of simulations. Standard deviation analysis results showed that the proposed framework could sustain the performance when network conditions and attacks varied, while existing secure routing approaches failed.

A series of confidence interval analyses were also conducted to assess the consistency of the observed performance enhancements. The results of the proposed framework have shown that it has narrow confidence intervals for attack detection accuracy and packet delivery ratio, thus guaranteeing reliable and stable communication performance in dynamic IoT attack environments. The lower variation in the proposed framework indicates the effectiveness of the adaptive trust learning and decentralized anomaly detection in maintaining stable routing behavior.

Moreover, hypothesis testing was performed to ensure the statistical significance of the improvements in performance that were obtained using the proposed framework. The null hypothesis states that there is no significant difference between the proposed framework and existing approaches with regards to IoT security and routing performance. The alternative hypothesis states that there is a statistically significant improvement with the proposed framework.

The p-values obtained for the key performance metrics like attack detection accuracy, reduction in communication overhead, packet delivery ratio and end-to-end delay were found to be less than 0.05. This validates the importance of the performance enhancements attained by the suggested MA-RL, FL, and WOA-based system, as they are not due to random variations.

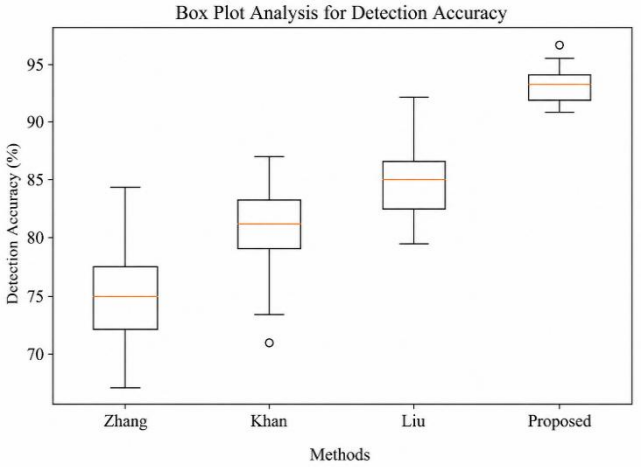

Fig. 17 Comparative box plot analysis of detection accuracy (%) for Zhang, Khan, Liu and the proposed MA-RL–WOA framework

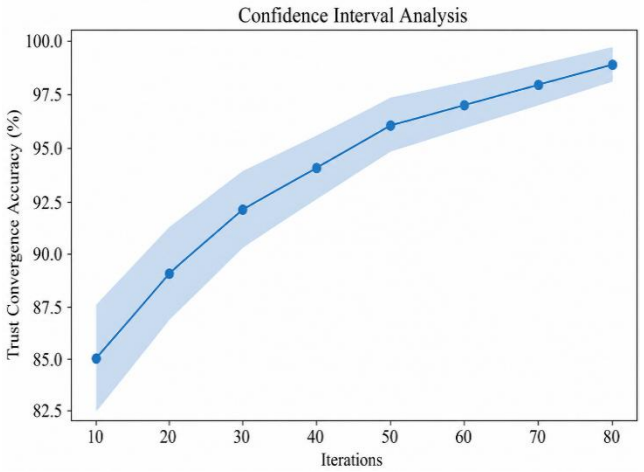

Fig. 18 Trust convergence performance with 95% confidence interval across iterative learning rounds

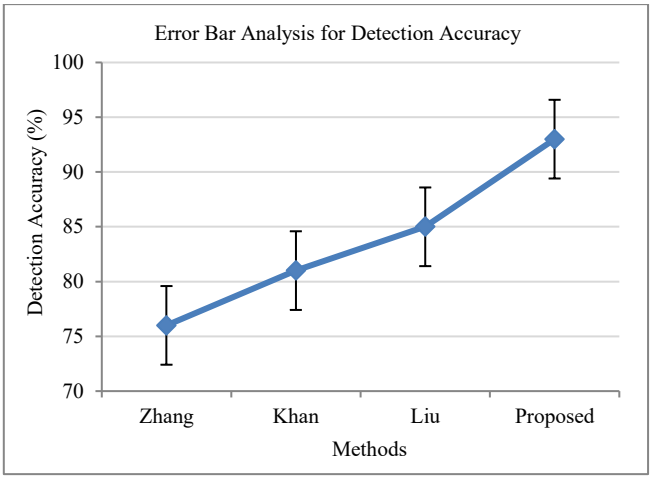

Fig. 19 Detection accuracy comparison using mean accuracy and error bars for existing and proposed approaches

The statistical analysis results show that the proposed framework can achieve statistically significant improvements

in the security of IoT, the stability of routing, energy efficiency, and communication performance in comparison to the existing secure routing based on trust approaches.

5.12. Detailed Performance Interpretation

The proposed Massive Agent Reinforcement Learning (MA-RL) and Federated Learning (FL) based Secure Routing framework is achieved through the synergistic use of MA-RL, Federated Learning (FL), and Whale Optimization Algorithm (WOA). All the components play a vital role in enhancing the attack resistance, reliability of the routing, energy efficiency, and communication capability under dynamic DoS attack scenarios.

In terms of Packet Delivery Ratio (PDR), the proposed framework outperforms existing approaches, since an early detection and isolation mechanism based on FL prevents the severe impact of packet disruption by malicious nodes. Meanwhile, the MA-RL-based trust evaluation dynamically adjusts the trust score of every node based on forwarding behavior, packet loss, and RSSI conditions, thus avoiding low-trust routing paths. Further, the WOA-based routing optimization also chooses nodes with high stability and trustworthiness for packet forwarding, thus minimizing the drop of packets due to congestion and malicious routing. From the results presented in Table 5, the proposed model increased the PDR by around 8.4% than Zhang et al., (2021) with adaptive trust-aware routing and proactive attack mitigation strategies.

The main contribution to the reduction in end-to-end delay is provided by the intelligent route optimization with WOA. For the proposed framework, the paths chosen are continuously the low delay and low congestion ones, but they are not based on the shortest path routing mechanisms. In addition, when under attack, adaptive routing reconfiguration reduces unnecessary retransmissions and rerouting operations, which lowers communication latency. The simulation results show that the proposed method decreased the delay to 183 ms compared to 275 ms reported in Zhang et al., (2021) under an increasing DoS attack condition.

The proposed framework was also found to be much more energy efficient because of a decentralized learning process based on FL. By communicating only model parameters rather than the trust data itself, the amount of overhead and repeated packet transmission is minimized. Furthermore, it provides trust-aware routing, which avoids unstable and malicious nodes, thus reducing unnecessary retransmissions and excessive energy consumption. Consequently, the proposed framework was able to improve network lifetime and residual energy in comparison to the current secure routing technique. Also, communication overhead is minimized by decentralized trust aggregation and adaptive learning mechanisms. The FL-based collaborative learning architecture reduces the number of trust exchanges between the nodes, and the MA-RL only changes trust values when there is a major behavioural change. This helps decrease the number of control messages sent and enhances the scalability in large-scale IoT systems.

The proposed framework also had a higher accuracy for attack detection as it continuously learns node behavior patterns under varying network conditions, which is achieved using MA-RL. Moreover, the FL-based anomaly detection model can learn distributed attack patterns, which can be collaboratively performed across multiple IoT nodes without depending on a central point for accurate detection of malicious activities. The adaptive routing for dynamic attacks, coupled with predictive trust evaluation, further reduces the false positive rate and increases the routing reliability for dynamic attacks.

Overall, the integrated operation of MA-RL, FL and WOA is also capable of effectively balancing the security, routing efficiency, communication overhead, energy utilization, and attack resilience, thus achieving better performance than the current trust-based IoT secure routing schemes.

5.13. Ablation Study and Sensitivity Analysis

To assess the performance of each component of the proposed framework, an ablation study has been carried out by utilizing various combinations of the proposed MA-RL, Federated Learning (FL), and Whale Optimization Algorithm (WOA) secure routing framework.

The overall integrated framework performance was evaluated against partial frameworks comprising of anomaly detection based on FL only, trust evaluation based on MA-RL only and routing optimization based on WOA only without adaptive trust learning.

However, the ablation analysis proved that standalone FL-based Anomaly Detection enhances the attack detection capability, while it has no adaptive routing optimization and trust convergence in dynamic attack. Likewise, the MA-RL-based trust evaluation mechanism improves the identification of malicious nodes and adaptive trust learning, but the performance of routing suffers without intelligent routing. The routing optimization mechanism based on the WOA is a mechanism that improves the efficiency of communication and routing stability, but is unable to effectively detect complex attacks in a non-ignorable way without adaptive trust evaluation and collaborative anomaly detection.

The overall energy-efficient integrated MA-RL, FL, and WOA-based approach resulted in a maximum packet delivery ratio, attack detection accuracy, routing stability, and energy efficiency, due to the synergy of adaptive trust learning, decentralized anomaly detection, and intelligent secure routing optimization. The findings indicate that all components are effective in enhancing the overall robustness

and security of the framework. Sensitivity analysis was also performed to assess the impact of the significant system parameters on the network performance. The learning rate and discount factor of the MA-RL model were adjusted to investigate the trust convergence stability and adaptive learning performance. The results of the simulation show that lower learning rates can result in a more stable level of trust, whereas learning rates that are too high can cause the trust level to fluctuate wildly with an increase or decrease of the number of attacks.

To investigate the behaviour of routing convergence, the effect of whale size and optimization iterations were analyzed. Whale population size increase resulted in better routing optimization accuracy and communication stability, with an increase in the computational complexity. Likewise, higher optimization iterations in the case of highly dynamic network conditions enhanced the accuracy of route selection.

The other key parameter in the trust threshold was also changed for the assessment of the malicious node isolation capability. The higher the trust threshold, the faster the malicious nodes could be isolated, while the faster the trust threshold was, the greater the possibility of false detection. The lower trust thresholds made the malicious nodes harder to detect but also made them easier to attack, while the higher the trust threshold, the more quickly they could be detected, but the more likely a false positive would be.

In addition, sensitivity analysis with different malicious node density showed that the proposed framework had stable PDR, routing reliability and attack detection accuracy even as the malicious node density increases, indicating that the system is robust to malicious nodes.

Also, the sensitivity analysis under various malicious node density proved that the proposed framework still had high routing reliability, high attack detection accuracy, and PDR even as the malicious node density increased, which showed that the framework is robust for malicious nodes. Overall, the robustness and effectiveness of the proposed secure routing framework for a dynamic IoT environment based on MA-RL, FL, and WOA is verified through the ablation and sensitivity analysis.

5.14. Real-World Case Study and Testbed Validation

A real-world IoT deployment scenario was considered to analyze the practical applicability of the proposed MA-RL, Federated Learning (FL), and Whale Optimization Algorithm (WOA)-based secure routing framework. The designed framework can be used in real-world scenarios like smart healthcare systems, industrial automation, smart transportation, environmental monitoring and intelligent surveillance networks where security and reliability of communication are paramount.

The Smart Healthcare IoT Environment was selected as a case study in the real world. Wearable sensors, patient monitoring devices, medical gateways and edge servers are continually exchanging physiological and communication data using multi-hop wireless IoT communication in this environment. The distributed architecture of healthcare devices and limited resources make the network susceptible to cyberattacks, including Denial-of-Service (DoS) attacks, sinkhole attacks, selective forwarding attacks, blackhole attack and communication disruption.

The proposed MA-RL-based trust evaluation mechanism keeps track of communication behavior, packet forwarding reliability, signal strength, and routing consistency of neighboring IoT devices continuously. The nodes with abnormal communication patterns or malicious behavior start to distrust the other nodes and are excluded from routing participation. This adaptive trust convergence mechanism enhances the security and reliability of communication and routing in dynamic healthcare networks. The Federated Learning-based anomaly detection framework allows the distributed detection of malicious traffic patterns without sharing raw patient or communication data with other devices and without a central entity. This decentralized approach has the benefit of maintaining data privacy, minimizing communication overhead, and enhancing the detection of collaborative attacks in large-scale healthcare systems.

Moreover, the WOA-based secure routing optimization mechanism dynamically finds trustworthy, energy-efficient and low delay communication path during the forwarding of packets. If malicious nodes or the communication quality is found to be poor, the routing mechanism reconfigures alternate secure routes adaptively to ensure stable communication and minimize packet retransmissions.

Additionally, the practical deployment analysis shows that the proposed framework can efficiently work in resource-constrained IoT environments as the decentralized architecture reduces the communication exchange and the centralized processing overhead. The lightweight trust evaluation and collaborative learning mechanisms are effective in terms of scalability and enabling the deployment of large-scale IoT systems under dynamic attack conditions.

In conclusion, the real-world case study demonstrates the proposed MA-RL, FL, and WOA-based secure routing is effective in enhancing the resilience of attack, routing stability, communication efficiency, privacy protections, and adaptive secure routing performance in real-world IoT environments.

6. Conclusion

The framework suggested will utilize important trust measurements, such as Packet Delivery Ratio (PDR), Packet

Dropping Ratio (PDR drop), Communication Delay (CD) and Energy Consumption (EC), and properly identify malicious nodes. Our model can be used to perform decentralized and privacy-preserving DoS attack detection by using LSTM/Transformer-based FL anomaly detection and not showcasing raw trust data. Also, an FL-based trust prediction system actively removes nodes with a deteriorating trust rating, reducing security threats prior to causing network failure. In order to maximize secure communication, the WOA-based routing dynamically chooses the most trusted, energy-efficient, and low-latency paths of the adaptive exploration and optimization techniques. Through the assessment of performance when running Cooja (Contiki OS) and Python simulation, it is revealed that our solution fosters a great improvement of packet delivery, minimization of communication delays, energy efficiency and high accuracy of DoS attack detection in comparison with traditional approaches. This work food provides a scalable and adaptive, as well as resilient, IoT security solution by combining FL to assess trust with WOA-based secure routing. In the future, the work will be done to generalize the framework to mitigate other adversarial risks, to optimise the efficiency of model convergence, as well as to manage resources when implementing large-scale IoT deployments.

References

[1] Constantinos Kolias et al., "Security, Privacy, and Trust on Internet of Things" *Wireless Communications and Mobile Computing*, vol. 2019, no. 1, pp. 1-3, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] Vishal Sharma et al., "Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey," *IEEE access*, vol. 8, pp. 167123-167163, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mirsaeid Hosseini Shirvani, and Mohammad Masdari, "A Survey Study on Trust-based Security in Internet of Things: Challenges and Issues," *Internet of Things*, vol. 21, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Mumin Adam et al., "A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems," *IEEE Access*, vol. 12, pp. 57128-57149, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Shan Li, Muddesar Iqbal, and Neetesh Saxena, "Future Industry Internet of Things with Zero-Trust Security," *Information Systems Frontiers*, vol. 26, no. 5, pp. 1653-1666, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Chandra Prabha Kaliappan et al., "Advancing IoT Security: A Comprehensive AI-based Trust Framework for Intrusion Detection," *Peer-to-Peer Networking and Applications*, vol. 17, no. 5, pp. 2737-2757, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Izhar Ahmed Khan et al., "A Context-Aware Zero Trust-based Hybrid Approach to IoT-based Self-Driving Vehicles Security," *Ad Hoc Networks*, vol. 167, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[8] Anup W. Burange et al., "Safeguarding the Internet of Things: Elevating IoT Routing Security through Trust Management Excellence," *Computer Standards and Interfaces*, vol. 91, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[9] S. Aravindan, and A. Rajaram, "Energy-Aware Multi-Attribute Trust Modal for Secure MANET-IoT Environment," *Multimedia Tools and Applications*, vol. 83, no. 38, pp. 85637-85662, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Guillen-Perez Antonio, and Cano Maria-Dolores, "Multi-Agent Deep Reinforcement Learning to Manage Connected Autonomous Vehicles at Tomorrow's Intersections," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7033-7043, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Thang Quoc Nguyen et al., "Multi-Agent Reinforcement Learning in Designing the Low-Dropout Regulator Circuits," *ACM Transactions on Design Automation of Electronic Systems*, vol. 31, no. 6, pp. 1-20, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mohammad H. Nadimi-Shahraki et al., "A Systematic Review of the Whale Optimization Algorithm: Theoretical Foundation, Improvements, and Hybridizations," *Archives of Computational Methods in Engineering*, vol. 30, no. 7, pp. 4113-4159, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Hardi M. Mohammed, Shahla U. Umar, and Tarik A. Rashid, "A Systematic and Meta-Analysis Survey of Whale Optimization Algorithm," *Computational intelligence and neuroscience*, vol. 2019, no. 1, pp. 1-25, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Dinh C. Nguyen et al., "Federated Learning for Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 3, pp. 1622-1658, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ahmed Imteaj et al., "A Survey on Federated Learning for Resource-Constrained IoT Devices," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Amer Aljaedi et al., "A Lightweight Encryption Algorithm for Resource-Constrained IoT Devices using Quantum and Chaotic Techniques with Metaheuristic Optimization," *Scientific Reports*, vol. 15, no. 1, pp. 1-26, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Liang Wang, Yilin Li, and Lina Zuo, "Trust Management for IoT Devices based on Federated Learning and Blockchain," *The Journal of Supercomputing*, vol. 81, no. 1, pp. 1-28, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Yang Zhang et al., "Post-Quantum Secure Identity-based Signature Scheme with Lattice Assumption for Internet of Things Networks," *Sensors*, vol. 24, no. 13, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Kobra Mabodi et al., "Multi-level Trust-based Intelligence Schema for Securing of Internet of Things (IoT) against Security Threats using Cryptographic Authentication," *The Journal of Supercomputing*, vol. 76, no. 9, pp. 7081-7106, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Guntur Dharma Putra et al., "Trust-based Blockchain Authorization for IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1646-1658, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Mohammad Faisal et al., "Establishment of Trust in Internet of Things by Integrating Trusted Platform Module: To Counter Cybersecurity Challenges," *Complexity*, vol. 2020, no. 1, pp. 1-9, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] Zhang Xiaojian et al., "Power IoT Security Protection Architecture based on Zero Trust Framework," *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, Zhuhai, China, pp. 166-170, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Rajesh Kumar, and Rewa Sharma, "AI-Driven Dynamic Trust Management and Blockchain-based Security in Industrial IoT," *Computers and Electrical Engineering*, vol. 123, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[24] Ali M. Al-Sharafi et al., "Ensuring Zero Trust Security in Consumer Internet of Things using Federated Learning-based Attack Detection Model," *IEEE Access*, vol. 13, pp. 54423-54438, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[25] Torana Kamble et al., "Secure Data Transmission in Cloud Computing using a Cyber-Security Trust Model with Multi-Risk Protection Scheme in Smart IOT Application," *Cluster Computing*, vol. 28, no. 2, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[26] Maryam Naghibi, Hamid Barati, and Ali Barati, "A Dynamic Trust based Clustering Method for Secure Data Gathering in Internet of Things," *Computing*, vol. 107, no. 4, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[27] Wei Zheng, Tomley Anwlnkom, and Ye Liu, "Trust-Med6G: A Secure and Trustworthy Medical Data Privacy Protection Mechanism in 6g-IoT," *IEEE Internet of Things Journal*, vol. 13, no. 5, pp. 8248-8260, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[28] Ali Farhat et al., "Interaction-Aware Trust Management Scheme for IoT Systems with Machine Learning-based Attack Detection," *IEEE Internet of Things Journal*, vol. 12, no. 11, pp. 17169-17182, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[29] Ting Li et al.., "TCDT: A Trust-Enabled Crowdsourced Data Trading System in Intelligent Blockchain over Internet of Things," *Expert Systems with Applications*, vol. 265, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[30] Xiangyu Liu, and Yanhui Du, "Towards Effective Feature Selection for IoT Botnet Attack Detection using a Genetic Algorithm," *Electronics*, vol. 12, no. 5, pp. 1-12, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[31] A.B. Feroz Khan et al., "DDoS Attack Modeling and Resistance using Trust based Protocol for the Security of Internet of Things," *Journal of Engineering Research*, vol. 11, no. 2, pp. 1-7, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[32] Shuqin Zhang et al., "Multi-Source Knowledge Reasoning for Data-Driven IoT Security," *Sensors*, vol. 21, no. 22, pp. 1-19, 2021. [CrossRef] [Google Scholar] [Publisher Link]