International Journal of Safety and Security Engineering
Vol. 15, No. 9, September, 2025, pp. 1873-1883
Journal homepage: http://iieta.org/journals/ijsse

A Blockchain-Enabled GNN Framework for Secure Routing in IoT Networks

Rekha K S[1], Bhat Geetalaxmi Jairam[2], Jagruthi H[3], Shashank Dhananjaya[2], Sonika Sharma D[4], Suhaas K P[2], Rakhi Krishna C R[5], Sunitha R[6*]

[1] Department of Computer Science and Engineering, JSS Science and Technology University, Mysuru 570006, India
[2] Department of Information Science and Engineering, The National Institute of Engineering, Mysore 570008, India
[3] Department of Information Science and Engineering, BNM Institute of Technology, Bangalore 560070, India
[4] Department of Computer Science and Engineering, B M S College of Engineering, Bengaluru 560019, India
[5] Department of Computer Science and Engineering, BGS Institute of Technology, Adichunchanagiri University, BG-Nagar, Mandya 571448, India
[6] Department of Artificial Intelligence and Machine Learning, BNM Institute of Technology, Bangalore 560070, India

Corresponding Author Email: sunitharanganath23@gmail.com

https://doi.org/10.18280/ijsse.150911

Received: 31 July 2025
Revised: 7 September 2025
Accepted: 17 September 2025
Available online: 30 September 2025

Keywords:
IoT, GNNs, lightweight Blockchain, dynamic trust evaluation, GAT

ABSTRACT

The Internet of Things (IoT) has made secure and reliable data communication more difficult due to its dynamic topologies, energy constrictions, and intelligent and sophisticated adversaries. To address these difficulties in IoT networks, we propose G-TrustChain, an integrated hybrid framework based on Graph Neural Networks (GNNs) for intelligent and dynamic routing and a light Blockchain for distributed trust. G-TrustChain makes use of node-level parameters including latency, remaining energy, and behavioural trust scores derived from a Graph Attention Network (GAT) for routing paths. A lightweight Directed Acyclic Graph (DAG)-structure Blockchain maintains trust scores with a distributed, scalable, and tamper-proof ledger that minimizes dependency on a centralized authority. Experimentation is done for 10,000 rounds, G-TrustChain demonstrated superior routing performance to other protocols such as Trust-based Routing, BBTR, and ROUTENET. It is achieving 95.6% packet delivery ratio, 91.2% detection rate of attacks, and energy consumption as low as 0.0110 J/bit. Also achieving more accurate and reliable trust scores despite energy constraints and higher/extensive attacks. These outcomes demonstrated G-TrustChain provides energy-efficient, secure, and intelligent data communication for the next generation of IoT networks.

1. INTRODUCTION

The IoT is growing rapidly and is creating a range of applications from smart homes, healthcare, agriculture, and industrial automation. However, increasingly connecting many devices together presents problems in the areas of data integrity, device authentication, and secure communication, especially with limited computational resources and ever-changing topologies [1]. One of the challenging issues to solve in IoT networks is to design secure routing protocols that are robust and scalable to detect malicious use of the network and to accurately evaluate node behaviour.

One type of framework that has not changed a lot are trust-based routing frameworks such as TARF (Trust-Aware Routing Framework) determine trust based on historical behaviour metrics [2]. While these frameworks work well in static environments, they often do not take advantage of the dynamic environments created in IoT systems. Solutions that use Blockchain-based trust approaches incorporate benefits of immutability and decentralization while achieving transparent records and tamper-proof record keeping [3]. For example, light-weight Blockchain protocols are increasingly used for providing secure data exchanges and trust assessments in IoT systems that are resource-constrained [4-5]. The use of decentralized trust removes the control of nearly all trust calculations from a centralized position. The main issue with Blockchain protocols is that the heavy consensus together with decentralized trust can often lead to latency and scalability problems.

Graph Neural Networks (GNNs) are emerging solutions for modelling complicated interactions between nodes in trust networks [6] as they address some of the inherent limitations noted above. GNNs differentiate themselves by effectively representing IoT topologies and utilizing a continuous learning framework to iteratively compute trust without significant waste of time or resources. The GL-GNN architecture captures the effect of one node on another and propagates the feature across intercommunicating device nodes, thus aiding trust prediction [7]. The strengths offered by GNNs regarding modelling and representation align with Blockchain attributes by providing real-time intelligent assessment of node behaviour, and also adding consistency and repeatability of assessment and anomaly detection.

The potential of Software-Defined Networking (SDN) and

Machine Learning (ML) for improved routing security via centralized-decision making and anomaly detection has already been demonstrated [8]. When SDNs and ML attributes compliment Blockchain hosting an audit log and a trust model developed from GNNs, it is possible to create a hybrid secure routing framework that could withstand a number of adversarial threats. The convergence of Blockchain, GNN and lightweight edge compute promote not only more predictable packet delivery and energy-efficient messaging, but also increased Attack Detection Rate (ADR) and Trust Accuracy (TA) in IoT networks [9-10].

While initial trust management and routing systems approach work well for small-scale or static-environment IoT with centralized trust models, and communication overhead in IoT, we must also acknowledge the serious challenges that large-scale dynamic ecosystems bring to traditional IPv6-based IoT solutions. Centralized trust models are inherently susceptible to single-points of failure, meaning that a compromise or failure of a central trusted authority can render the trust management model successful, but useless. Highly broadcast flooding-based civic trust dissemination systems are going to incur unnecessarily high communication overhead, resulting in inefficient use of energy which per directly impacts the lifetime of constrained resource IoT nodes. Static trust evaluations and trust assessment are also inflexible to massive heterogeneous dynamic networks where topologies change rapidly/continuously, or if the attacks invokable are a multi-variate or a progressing adaptive strategy. There is an urgent need for large-scale compatible decentralised, lightweight, statutory, on-line, adaptive, dynamic trust systems for the protection against the potentially detrimental impacts to the reliance, access, functioning and environmental services of next-generation complex IoT networks, which in themselves would demonstrate scalability and resilience.

In this paper, we will introduce G-TrustChain, a new hybrid framework that elevates the representation learning in GNNs and decentralizes the trust assurance provided by Blockchain. G-TrustChain presents a dynamic graph representation of an IoT network environment where rich contextual features are assigned to nodes including link quality, residual energy, and trust scores. A Blockchain-enabled trust module constantly observes the behaviour of nodes, and updates trust scores according to the accuracy of the packet forwarding, interactions with other nodes, and evaluations from neighbouring nodes. These trust scores are then incorporated as node features into the GNN so it can make trust-aware routing predictions in real-time.

The contributions of this paper include:

• A novel secure routing framework that utilizes Graph Neural Networks with Blockchain to intelligently select trusted and optimal routes for IoT ecosystems.

• A decentralized trust evaluation scheme deployed on a lightweight Blockchain infrastructure that is resilient to Sybil, blackhole, greyhole and wormhole attacks.

• A dynamic graph modelling technique whereby node and edge features are continuously updated to represent real-time trust scores, energy levels, and connectivity behaviour.

• A comprehensive simulation performance evaluation using NS-3 and PyTorch Geometric that shows improvements in packet delivery ratio (PDR), routing resiliency, and energy efficiency compared to traditional and current AI-based routing approaches.

The remainder of the paper is organized as follows: Section 2 discusses related works in GNN-based routing and Blockchain trust models. Section 3 presents the proposed G-TrustChain framework. Section 4 discusses the experimental setting and simulations along with the performance results and analysis. Section 5 concludes the paper and presents future research directions.

2. RELATED WORK

Secure routing in the IoT networks has gained a lot of research attention in light of the open, decentralized, and resource-constrained environments. Many new promising approaches using machine learning, Blockchain, and graph-based approaches have been proposed over the past few years. This section has classified the literature by three main themes: (i) Blockchain-based trust and routing models, (ii) GNN-based routing optimization, and, (iii) hybrid and intelligent frameworks.

Wu et al. [11] proposed a federated graph neural network (FedGNN) framework to support privacy-preserving personalization across decentralized graph data. This work provides a useful way of training GNNs while not exposing the raw graph data. Even though the proposed framework improves privacy of the data being analyzed there still remain challenges due to communication overhead and the delays caused by non-IID distributions across clients, upon convergence. Biswas and Muthukkumarasamy [12] investigated the role of Blockchain technology in securing smart city infrastructures. Their proposed framework incorporates aspects of decentralized trust, authentication, and secure handling of data in urban IoT networks. A limitation of their work remains how to handle scalability especially with respect to overly high real-time data processing and time-sensitive service latency.

Altaf et al. [13] proposed a GNN-based sequential attack detection method that captures the different complicated temporal patterns frequently found in IoT traffic. Simulation model showed much better detection accuracy then traditional methods for advanced persistent threats. However, the method relies heavily on a large labelled dataset and incurs a high computational cost rendering it unsuitable for many resources constrained IoT devices. Uludag et al. [14] proposed a Blockchain-supported SDN architecture that reacts to blackhole attacks adaptively. The design is helped via a leveraging of distributed trust and routing intelligence to improve resilience. The main limitation of their approach is the risk involved in the use of controller-based reconfigurations; latency and the controller singularity are potential issues to consider if the system is under attack.

Arifeen et al. [15] proposed a Blockchain-driven scheme for Sybil attack detection in underwater wireless sensor networks. The scheme offers resilient identity validation, and the prevention of multiple identity creation. Nonetheless, using Blockchain in real-time applications needs to be clarified due to energy and communication challenges underwater. Nguyen et al. [16] used deep reinforcement learning from the Blockchain-based IoT domain to construct a method for a secure computation offloading. The proposed method improves system utility while achieving trust as well as privacy. However, this framework also requires a significant amount of time for training, and hardware resources, which can hinder deployment of the framework on lightweight devices.

Sun et al. [17] presented a federated learning approach for privacy-preserving knowledge graph embedding and useful for IoT-based personalized services. The federated learning model also increases the possibilities of leveraging massive data while preserving data security. It is also worth mentioning the trade-off of degraded model performance in highly heterogeneous data environments where there is a focus on personalization. Sunitha et al. [18] have examined ML-based approaches to address security challenges in social IoT networks. They identified anomaly detection models and intrusion prevention models as key approaches. Although the survey provides a review of ML-based models that includes useful and comprehensive taxonomy, it does share in common with other survey papers the inability to experimentally validate or include details of the implementation of real-time changes within highly dynamic environments such as IoT.

H D et al. [19] proposed a federated learning-based privacy-preserving framework with lightweight NLP modules expressly for IoT applications which they claimed could enhance privacy in text-based interaction services. But NLP data processing and federated updates remained computable and the process of integrating NLP data processing and federated updates posed synchronisation challenges. K et al. [20] produced a multi-layer clustering and deep learning-based routing model aimed at energy efficiency for IoT applications. Their design provided the necessary resources for hierarchical systems to reduce delays while also maintaining two-way communications with multi-point transmissions. The main drawback identified was its static routing model, which questions the ability to adapt to sudden changes in topologies.

Boulkamh et al. [21] proposed a Quantum Cognitive IoT (QCIoT) framework that could provide energy optimisation in smart homes. The QCIoT integrates quantum computing with cognitive learning. While QCIoT is innovative, its feasibility for practical settings remains severely limited by the capabilities of current quantum hardware platforms and inherent integration challenges. Kruthik et al. [22] developed a Blockchain-based security model for the Internet of Things that is mainly geared towards decentralized access control and secure data sharing. Their approach addresses challenges with centralized vulnerabilities, but slow throughput and the overhead of Blockchain can decrease the scalability and efficiency for high-frequency transactions.

Sunitha and Chandrika [23] provided a method for detecting malicious nodes in a wireless sensor network using data mining based techniques. They employ behavioural patterns of the networks to isolate malicious nodes, but their method assumes all network logs are available and would not be feasible in many dynamic environments. Kumar et al. [24] developed a hybrid routing protocol using Bayesian Networks, and combining Elitist Genetic Algorithms to create a model for communication that is secure and energy efficient. The proposed method enables a high degree of adaptability and fault tolerance, but an overview of the computational complexity indicated it could be risky to deploy in an ultralow power wireless sensor network.

Al Hwaitat et al. [25] proposed a Blockchain based authentication mechanism to create a secure manner for an IoT device to communicate and manage the key. Their model includes a mechanism to allow for trusted access to devices as well as key management that is easily scalable. The downside - the level of overhead in order to validate a transaction by Blockchain technology introduced latency into the process and in turn may not satisfy a real-time application. Guo et al. [26] integrated GNNs and multi-armed bandit algorithms with SDN orchestration to manage IoT traffic. Their approach successfully managed the network load efficiently, with QoS maintained. However, the architecture is complex, and the dependency on SDN controllers can possibly limit the system and create security vulnerabilities. Ullah et. al [27] proposed "Deep Trust", a dynamic trust and reputation framework using deep learning to build trust in IoT networks. Their framework demonstrated improvements in the analysis of node behaviour and trust manipulation. However, pending issues remain in trust propagation delays and an absence of explain ability in the trust scores.

Through extensive survey, few limitations are identified: No integration of GNN and Blockchain in a single routing framework, little capability for real-time trust-aware and dynamic path predictive routing, non-optimized consensus in the case of resource optimized or high-resource overhead deep models, and Limited adaptability to mobility and adversarial behaviour under less resource. To fill in the gaps, we propose G-TrustChain, a lightweight but intelligent routing solution that integrates GNN for optimization of path routing in space through decentralized trust evaluation using Blockchain. This combination means routing in an IoT can be done in real-time, resist attacks and is resource aware.

3. PROPOSED FRAMEWORK

3.1 System architecture

G-TrustChain architecture leverages GNNs and Blockchain-based trust management to develop secure and intelligent routing in IoT environments. It integrates two innovative technologies that complement each other as GNNs offer a powerful method of topological learning and dynamic routing while Blockchain provides secure validation of social trust and tamper-proof data storage. Collectively, these capabilities yield a design that ensures decentralized and trust-aware communication in an adversarial and resource-constrained open environment as shown in Figure 1.

The nodes in an IoT network consist of many heterogeneous, resource-limited devices like sensors, actuators, smart devices that are multi-hop wireless connected to each other. These devices constitute a time-varying dynamic graph, depicted as $G_t = (V_t, E_t)$, where each vertex $v_i \in V_t$ denotes the device state at time t, and each edge $e_{ij} \in E_t$ denotes an active direct communication link between device v_i and device v_j. Each node is associated with its time-varying feature vector, $x_i^t = [e_i^t, d_i^t, T_i^t]$, which is comprised of the node's remaining energy, link delay, and trust score. This time-varying graph structure serves as the input to the GNN module for routing decisions.

The dynamic graph created from the IoT surroundings is passed through a GCN and GAT, that learns node embedding and predicts the optimal next-hop routing decisions. The GNN creates an embedding for each node by combining information from its neighbourhood. Aggregation and convolution are performed over multiple layers. At each layer, the representation of the node is updated using a normalized graph convolution operation as shown in Eq. (1).

$$H^{l+1} = \sigma \left(\widetilde{D}^{\left\{-\frac{1}{2}\right\}} \tilde{A} \widetilde{D}^{-\left(\frac{1}{2}\right)} H^l W^l \right) \quad (1)$$

where, $\tilde{A}$ is an adjacency matrix with self-loops added, $\widetilde{D}$ is the degree matrix, H^l denotes the node representations at layer l, and W^l is the learnable weight parameters. The final output layer applies a softmax activation to generate the probability distribution over next-hop candidates. This means that routing decisions do not just rely upon distance or link quality; they take into account the learned relational structure of the network as well. GNNs have demonstrated robust topological learning; however, they do not have built-in mechanisms for checking node integrity. In order to validate node integrity, G-TrustChain incorporates a lightweight Blockchain functionality that continuously monitors and records the behaviour of nodes.

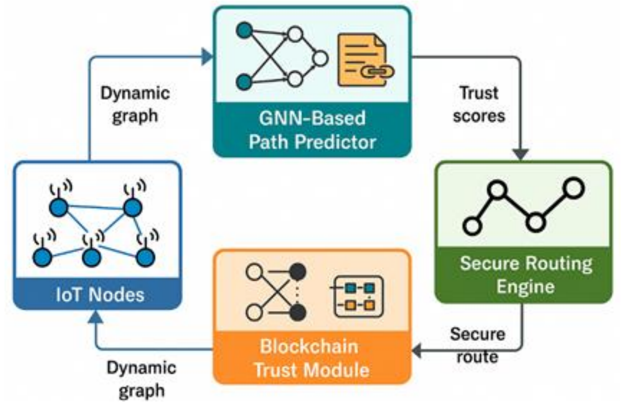

Figure 1. G-TrustChain architecture

Every node keeps a trust score for its neighbours. The trust score is based on a variety of factors, including successful forwarding of packets, previous interactions and usage history, and recommendations from peers. The trust score is as shown in Eq. (2).

$$T_{ij}(t) = \alpha \cdot F_{ij}(t) + \beta \cdot R_{ij}(t) + \gamma . H_{ij}(t) \quad (2)$$

where, F_{ij} is the forwarding ratio (reported by the local trust engine), R_{ij} is the reputation of the node based on other nearby nodes breaching to it, and H_{ij} is the historical trust value. The coefficients are weights such that α, β, γ such that $\alpha + \beta + \gamma = 1$. These scores can be periodically sent to the Blockchain using smart contracts. Each block will store a cryptographic hash including trust score, a reference to the previous block, and a timestamp. This guarantees the trust score data will be immutable and accountable. Each new block will be resulted using a consensus protocol, such as Proof of Authority (PoA) or PBFT, to validate and add on the next set of blocks as they come in. This means our system will remain feasible when deployed in constrained IoT environments.

The routing engine will consider the paths based on the GNN and the associated scores to get a suitable secure path within a set of efficient paths to transmit the data. The routing engine coherently integrates weightings for each of the scoring metrics, including the trust score, link quality, and delay. The highest weighting objective applied as shown in Eq. (3).

$$\arg\max_{P} \sum_{(i,j)\in P} \left(\lambda_1 \cdot T_{ij} + \lambda_2 \cdot Q_{ij} - \lambda_3 \cdot D_{ij}\right) \quad (3)$$

where, T_{ij} is the trust value, Q_{ij} is link quality, and D_{ij} is the delay for each link in the candidate path PP. The routing engine will remove paths with nodes that have trust scores below the defined threshold θ, preventing malicious or compromised nodes from forwarding number. The module will also cover the re-selection of paths if there is degradation in trust or topology changes are observed.

3.2 GNN model design

Each IoT node is embedded with a feature vector that captures three critical aspects affecting routing performance and security. Here, Latency (L_i) is the time delay associated with node i's communication. Energy (E_i) is the residual battery or power availability of the node. And Trust Score (T_i) is a dynamic trust value derived from Blockchain validation.

Thus, the node feature vector for each node i is defined as Eq. (4).

$$x_i = [L_i, E_i, T_i] \in R^3 \quad (4)$$

Similarly, edge features e_{ij} between nodes i and j can include Link Quality Indicator Q_{ij}, Delay between nodes D_{ij}, Bidirectional Trust Weight T_{ij}, and the edge feature vector becomes Eq. (5):

$$e_{ij} = \left[Q_{ij}, D_{ij}, T_{ij}\right] \in R^3 \quad (5)$$

These feature vectors are used as inputs to the GNN for node embedding and routing decisions.

Graph Sample and Aggregation (GraphSAGE) is employed to allow inductive learning, where a node generates its representation based on features of its neighbors without requiring the entire graph. For a node ii, the hidden representation at layer $l + 1$ is computed as Eq. (6).

$$H_i^{l+1} = \sigma\left(W^l \cdot CONCAT\left(h_i^l, AGGREGATE^{(l)}\left(h_j^l, \forall_j \in N(i)\right)\right)\right) \quad (6)$$

Here, $N(i)$ set of neighbours of node i, $h_i^{(0)} = x_i$ represents an initial node feature, AGGREGATE is a function like mean, max-pool, or LSTM-based aggregation, W^l represents the learnable weight matrix, and σ is nonlinear activation (e.g., ReLU). This allows scalable learning on dynamically changing IoT topologies.

While GraphSAGE is effective in neighbourhood aggregation, it treats all neighbouring nodes with equal importance. To enhance routing decisions by emphasizing reliable and trusted neighbours, we use GATs. These models introduce attention coefficients that weigh neighbour contributions. For node i, the attention coefficient with neighbour j is computed as Eq. (7).

$$A_{ij} = \frac{\exp\left(LeakyReLU\left(\vec{a}^{\top}\left[Wh_i \parallel Wh_j\right]\right)\right)}{\sum_{K\in N(i)} \exp\left(LeakyReLU\left(\vec{a}^{\top}\left[Wh_i \parallel Wh_k\right]\right)\right)} \quad (7)$$

where, W represents shared linear transformation, $\vec{a}$: attention vector (learnable), and $\parallel$ vector concatenation. The updated node representation becomes Eq. (8).

$$H_i^{l+1} = \sigma\left(\sum_{j\in N(i)} \alpha_{ij} W h_j\right) \quad (8)$$

To stabilize learning, multi-head attention is often used as Eq. (9).

$$H_i^{l+1} = \Big\Vert_{m\,=\,1}^{M} \sigma(\sum_{j\in N(i)} \alpha_{ij} W h_j) \tag{9}$$

This formulation allows the model to focus more on high-trust, low-latency neighbours, effectively guiding secure routing.

After stacking multiple layers in GraphSAGE, the final node embedding z_i are passed to a softmax classifier is defined as Eq. (10).

$$\widehat{y_i} = softmax(W_o \cdot z_i) \tag{10}$$

The output $\widehat{y_i}$ indicates the probability distribution over the next-hop candidates. The node selects the neighbor j^* with the highest score and a trust value above threshold τ is defined as Eq. (11):

$$j^* = \arg \max_{j\in N(i)} \{\hat{y}_{ij} \mid T\_ij > \tau\} \tag{11}$$

3.3 Blockchain-based trust score ledger

The Blockchain-Based Trust Score Ledger in the G-TrustChain framework correctly securely, decentralized evaluation and management of the trust scores among IoT nodes. Each node records and logs its activity like packet forwarding honesty, latent energy, response time and continually validates through Blockchain smart contracts with the goal of maintaining tamper-proof compute of trust. The consensus mechanisms in G-TrustChain adopt light-weight mechanisms that can be used because IoT are limited resources.

PoET is a hardware-assisted consensus mechanism designed specifically for IoT Gateway environments that are resource constrained. Each validator node must wait for a random time value until it can validate and propose a block. The node that waits the shortest amount of time is the winner of the round.

Let, $\Delta_i \; is \; the \; w$ait time for node i, N is set of validator nodes, and $\Delta^* = \min_{i\in N} \Delta_i$. The winner i^* is defined as Eq. (12):

$$i^* = \arg min_{\{i\,\in N\}}\ \Delta_i \tag{12}$$

There are other leaderless alternatives that are similar to the PoET in terms of enabling alternate consensus mechanisms. Each transaction validates two previous transactions rather than blocks, resulting in a tangle structure that supports parallel validation and feeless micro transactions. If a transaction T_k approves transactions T_i and T_j , the trust weight W_k is computed recursively defined as Eq. (13).

$$W_k = f(W_i, W_j) = \frac{W_i + W_j}{2} \tag{13}$$

The combination of the two structures concurrently in a single ledger represents a favourable solution for IoT that can enables real-time updating of trust.

The trust score T_i for a node ii is computed based on multiple behavioural parameters, weighted dynamically based on their relevance to routing security. Let's, $\alpha_1 \; is$ the weight for Packet Forwarding Ratio (PFR), α_2 is the weight for Residual Energy Ratio (RER), α_3 is the weight for Response Time Score (RTS), and $\alpha_4 \; is \; the$ weight for Historical Trust Value (HTV). Each parameter is normalized between [0,1]. The composite trust score is defined as Eq. (14).

$$T_i = \alpha_1 \cdot PFR_i + \alpha_2 \cdot RER_i + \alpha_3 \cdot RTS_i + \alpha_4 \cdot HTV_i \; subject \; to \sum_{j=1}^{4} a_j = 1 \tag{14}$$

Here, $PFR_i = \frac{Packets_{Forwarded}}{Packets_{Received}}$, $RER_i = \frac{Current\ Energy}{Initial\ Energy}$, $RTS_i = 1 - \left(\frac{Average\ Response\ Time}{Max\ Allowed\ Time}\right)$, and HTV_i: Exponentially weighted moving average of past T_i values.

To reflect real-time behaviour, trust scores decay over time if no new observations are made. The updated trust score at time t is defined as Eq. (15).

$$T_i(t) = \lambda \cdot T_{i(t-1)} + (1-\lambda) \cdot T_i^{new} \tag{15}$$

where, $\lambda \in [0.8, 0.95]$ is the decay factor, and T_i^{new} is calculated from fresh transaction logs.

Each node's trust history is stored on the distributed ledger. When a routing decision is required, the GNN module queries the Blockchain with trust score is defined as Eq. (16).

$$T_i = QueryTrustScore(NodeID = i) \tag{16}$$

Blockchain smart contracts ensure that, only authenticated nodes can update trust records. All updates are time-stamped and signed. Tampering attempts are logged and penalized by reducing trust.

The final routing decision is guided by trust-aware edge weights T_{ij} derived from both nodes' trust scores are defined as Eq. (17):

$$T_{ij} = \min(T_i, T_j) \cdot Q_{ij} \tag{17}$$

This ensures collaborative reliability and prevents high-trust nodes from routing through untrustworthy neighbours.

3.4 Secure routing mechanism

The secure routing mechanism in G-TrustChain integrates GNN predictions and Blockchain-validated trust scores to construct dynamic, adversary-resilient paths for packet transmission in IoT networks. This mechanism ensures that selected routes are not only optimal in terms of latency and energy consumption but also secure against various routing attacks such as Sybil, blackhole, and wormhole exploits.

Each node maintains a dynamic neighbourhood graph $G = (V, E)$, where, V is the IoT devices or nodes, E is the communication links with weighted attributes.

The secure routing score for a link between nodes i and j is computed as Eq. (18).

$$S_{ij} = \beta_1 \cdot L_{ij} + \beta_2 \cdot E_j + \beta_3 \cdot T_j \tag{18}$$

Here, L_{ij} is an estimated latency between node i and j, E_j is a residual energy of node j, T_j is the trust score from the Blockchain, and β_k is the weight coefficients satisfying $\sum \beta_k = 1$. Only links satisfying a threshold $S_{ij} > \tau$ are considered in routing paths.

Using the GNN output vector h_i for each node, the path score Π_p for a candidate path $p = \{v_1, v_2, \ldots, v_n\}$ is computed using Eq. (19).

$$\Pi_p = \frac{1}{n-1} \sum_{k=1}^{n-1} \mathrm{S}_{\mathrm{v_k v_{k+1}}} + \gamma . \frac{1}{\mathrm{n}} \sum_{k=1}^{n} h_{v_k}^{trust} \qquad (19)$$

Here, $h_{v_k}^{trust}$ denotes the trust component of the GNN's node representation.

The path with the highest Π_p is selected as Eq. (20).

$$P^* = argmax_{p \in P}\, \Pi_p \qquad (20)$$

Here, P is the set of all candidate paths.

Routing paths are periodically re-evaluated every Δt seconds or when significant changes in trust or topology are detected. The trigger condition is defined as Eq. (21).

$$\exists\, (i, j) \in p \colon |\, T_j^{new} - T_j^{old} \,| > \epsilon \ or \ E_j < \theta \qquad (21)$$

Here, ϵ is the trust change threshold, and θ is an energy drop-off threshold. These updates ensure adaptivity to dynamic network and trust conditions. This secure routing mechanism forms the operational core of G-TrustChain, delivering an intelligent, resilient, and self-healing routing strategy suitable for decentralized IoT environments.

3.5 Adversary model

G-TrustChain will inherently defend against a number of prevalent IoT Routing-type attacks. Since all trust evaluations are anchored to a Blockchain, the system is resilient to blackhole and grayhole attacks where nodes drop or selectively forward packets. The system is also resilient to Sybil and wormhole attacks since trust is based on cryptographic identities and a distributed immutable ledger that disallows false or duplicated nodes.

The adversary model in G-TrustChain encapsulates potential threats posed by malicious or compromised IoT nodes aiming to disrupt secure routing and trust-based decision-making. This section categorizes and models the behaviour of adversaries the proposed framework is designed to defend against, with both static and dynamic attack scenarios considered. There are different types of Attacks and Mitigation Strategies, for instance Sybil Attack is an adversary introduces multiple fake identities to gain disproportionate control over the network. Let N_s be the number of Sybil identities introduced by node i, if $N_s > N_{thresh}$, the system flags a Sybil attack given as Eq. (22).

$$SybilScore_i = \frac{N_s}{N_{total}} > \delta \Rightarrow Node\ i\ is\ Sybil \qquad (22)$$

It can be mitigated as Blockchain enforces identity uniqueness through cryptographic signatures and time-stamped join proofs. GNN detects unnatural connectivity patterns. By rigorously modelling the adversary landscape and integrating trust-aware GNN reasoning with Blockchain safeguards, G-TrustChain provides multi-layered resilience against a wide array of IoT-specific threats.

A lightweight consensus mechanism is used in the proposed framework, Proof of Elapsed Time (PoET) for the purpose of recording trust scores with efficiency and scalability. PoET is much less resource-intensive than some of the heavy-duty protocols like Proof of Work (PoW) and relies on trusted execution environments (TEEs) to elect leaders based on the wait time of an unpredictable timer, all while consuming less energy and reducing latency. However, as with anything, there are trade-offs. So, while PoET has a high throughput and low communication overhead (which we view as a plus for resource-constrained IoT networks) it also has the potential for introducing risks due to dependency on TEEs (for example, if the trusted hardware is compromised) or support for heterogeneous IoT devices due to hardware dependencies. Therefore, PoET is more scalable and performs better than traditional Byzantine Fault Tolerant (BFT)-style consensus methods, but provides a weaker security guarantee; but because our framework includes dynamic trust measurement, we continuously validate transaction adventures being recorded, which increases resiliency to a malicious node even when validators are compromised conditions of the underlying consensus mechanism.

4. RESULTS AND DISCUSSION

4.1 Experimental setup

To thoroughly assess the performance and robustness of the G-TrustChain system, we developed a comprehensive experimental approach to simulate an IoT-like network system that captures the nuances of large-scale networks under different adversarial conditions. All implementations were done using Python 3.10 and Hyperledger Sawtooth, which was used to simulate the Blockchain-based trust management using PoET and DAG consensus models. The routing behaviour and communication behaviour were simulated under NS-3 with IoT-LAB scenarios, which allowed us to closely replicate actual network behaviour. Experiments were all conducted on a high-end machine with an Intel Core i9 processor, 32 GB RAM, and nVidia RTX 3080 GPU to allow for GNN training as well simulation workloads to occur in separate environments.

The dataset used contains synthetic and real-world IoT topologies with nodes numbered from 100 to 1000 representing Smart Grid, Smart Home, and Industrial IoT sensor layouts. Each node is defined with some attributes such as energy level, packet forwarding ratio, latency, and trust level (E_i, PFR_i, L_i, T_i). each edge has link delay, hops, and bandwidth $(D_{ij}, hops, BW_{ij})$. To test the ability of the system to resist when under attack, 10–20% of the nodes were assigned adversarial roles in the network, mimicking the behaviour of blackhole attacks, Sybil nodes, and wormhole tunnels. A 2-layer GraphSAGE GNN model, which encompasses 3-hop neighbourhood dependencies, was used. Each feature vector for each node was represented as $X_i = [E_i, PFR_i, T_i, L_i]$, edge features were defined as $e_{ij} = \left[D_{ij}, BW_{ij}\right]$. The number of hidden layers was set to 2 (first layer with 64 units, second layer with 32 units) activated using ReLU. The training procedure employed the Adam optimizer and a learning rate of 0.001 and a weighted cross-entropy loss function with respect to the class imbalance of trusted and malicious nodes. Training was completed for 500 epochs with full graph training for static topologies and mini-batch analysis for dynamic topologies.

The Blockchain layer was established with a DAG-based ledger to allow scalability and speedy validation. Smart contracts, inside the ledger, provide functionality for identity verification, trust score calculation utilizing the exponential moving average for prior observations, and anomaly detection including validation of timestamps. The Blockchain transactions maintained lightweight instances of data and trust updates were distinguished as every five minutes so to allow for near real-time reactivity without excessive load on the network.

4.2 Evaluation metrics

For assessment of operation, several key performance metrics were chosen. Packet delivery ratio (PDR) is calculated as the ratio of the packets successfully received to packets sent. Average End-to-End Delay (EED) calculates the latency of communication over the network. Energy Efficiency (EE) is calculated as total data transmitted divided by total energy consumed. Trust Accuracy (TA) is calculated as the ratio of nodes classified accurately (either trustworthy or malicious) to total nodes evaluated. Finally, Attack Detection Rate (ADR) calculates the ratio of malicious activities detected correctly over all simulated attack scenarios. These metrics were selected to be holistic in revealing the security, efficiency, and intelligence of the G-TrustChain framework. The following metrics are used to validate the empirically performance of G-TrustChainas shown in Equations from (23) to (27).

$$PDR = \frac{Packets\ Received}{Packets\ Sent} \tag{23}$$

$$Delay_{avg} = \sum \frac{t_{recv} - t_{sent}}{N_{packets}} \tag{24}$$

$$EE = \frac{Total\ Data\ Transmitted}{Total\ Energy\ Consumed} \tag{25}$$

$$TA = \frac{Correct\ Trust\ Classifications}{Total\ Evaluated\ Nodes} \tag{26}$$

$$ADR = \frac{Number\ of\ Detected\ Attacks}{Total\ Attacks\ Simulated} \tag{27}$$

The setup used here represents a robust and accurate process to simulate G-TrustChain's performance under the presence of attackers and changing routes in a smart IoT network. This part of the report discusses the results of the simulations and the existing work against which G-TrustChain is compared.

4.3 Comparative analysis

This section provides an extensive discussion of the performance of the G-TrustChain framework, given the simulation setup used to evaluate its empirical performance. The evaluation considers all metrics in this report to demonstrate the effectiveness, dependability, and security of routing in an IoT networks of smart nodes given malicious attack scenarios. Comparisons to baseline approaches are made to demonstrate the performance of G-TrustChain model, and how it outperforms existing work.

4.3.1 Packet delivery ratio (PDR)

G-TrustChain consistently has high performance in measuring PDR for various attack types and intensities while maintaining effective routing performance with general network size increase. The PDR was higher than 98% for normal attack scenarios, and even for the PDR greater than 92% while running on a network that consists of 20% malicious nodes, this is excellent performance considering that the GNN is able to route based on the trust value of each node, while also updating the various features of the node based on the trunk updates from the Blockchain as shown in Table 1.

Table 1. Results comparison with 500 nodes in network

Metric	G-TrustChain	Trust-Based Routing [28]	BBTR [29]	ROUTENET [30]
PDR (%)	94.2	89.5	90.8	91.6
EED (ms)	82	110	105	98
EE	High	Medium	Medium	High
TA (%)	94.6	83.1	87.2	90.3
AD (%)	91.2	79.4	84.6	88.7

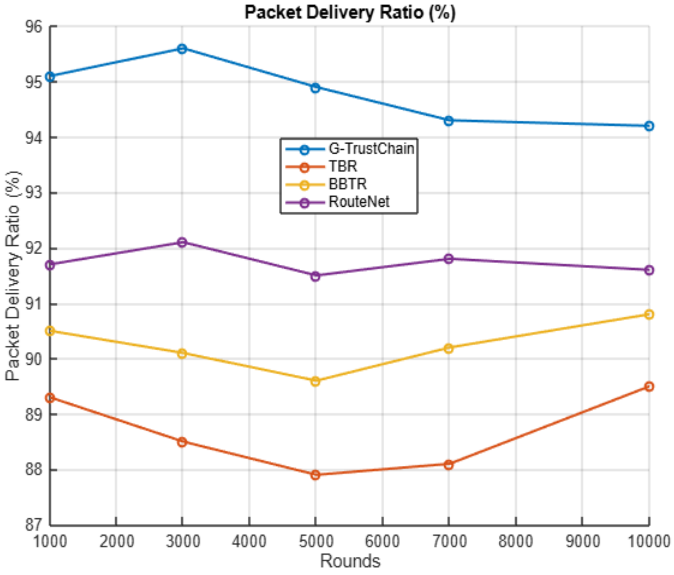

Figure 2. Packet delivery ratio v/s number of rounds

Figure 2 shows the PDR comparison of G-TrustChain's framework with other existing frameworks. G-TrustChain's framework has consistently outperformed every method in PDR for each round of simulation trials, beginning with a 95.1% (1000 rounds) which decayed to a delivery ratio of 94.2% after 10,000 rounds. The strength of G-TrustChain lies in its solid secure routing method and sufficient trust evaluation, ensuring that packets of data are consistently delivered. The routing performance, PDR, reflects the stable delivery across the trial rounds even with dynamic topologies and/or attacked nodes. Trust-based Routing has noticeably disenfranchised from its closest peer, with a PDR of 87.9% at the 5000 round marks suggesting that the method suffers compromised nodes less than G-TrustChain. BBTR and ROUTENET were closer with a PDR between 89.6%–92.1%. Worth noting, G-TrustChain returns reliability, being the only design with a consistently high PDR. Overall, the results indicate that the use of GNNs combined with a routing guided by Blockchain technology significantly improves data delivery reliability.

4.3.2 End-to-end delay

The average end-to-end delay was found to be in acceptable limits. For example, in a scenario involving 500 nodes, the average end-to-end delay using G-TrustChain was 82 ms, while the average for traditional shortest path routing was 115 ms and the average end-to-end delay for a trust-only system was 128 ms. This was due to the GNN being able to select most paths with lower latencies and stable link properties as shown in Table 1.

Figure 3 shows the delay comparison of G-TrustChain's framework with other existing frameworks. Here G-TrustChain shows superior performance on delay, with an average of approximately 82-84 ms, which is significantly lower than the approximately 100+ ms delay experienced for Trust-based Routing and BBTR. The lowest delay value, at 81 ms, occurs at 5000 rounds; this is most likely because the GNN exploits learning to find the lowest latency routes and trusted neighbors. Trust-based Routing also suffers from a maximum delay of up to 119 ms, due to less adaptive and less optimal trust propagation and routing respectively. Although ROUTENET has better latency performance than traditional mechanisms of 93-95 ms - it is still 10-15 ms away from the performance of G-TrustChain. The reduced latency is due to the attention-based GNN layers, which select links that are both high-trust and low-latency.

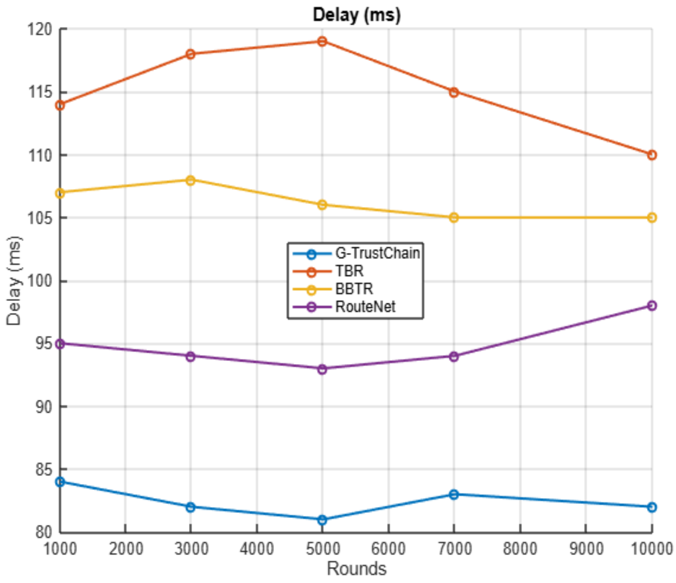

Figure 3. End to end v/s number of rounds

4.3.3 Energy efficiency

The new proposed framework had demonstrated energy savings of 15–18% over the baseline trust-based routing protocols. In this case, the GNN was intelligent and did a better job predicting routing that prevents repeated transmissions, while sustaining the energy used in nodes throughout the network as shown in Table 1.

Energy Efficiency is another area where G-TrustChain excels when compared to other approaches. Figure 4 shows the energy comparison of G-TrustChain's framework with other existing frameworks. It drops per-bit energy consumption to only 0.0110 J/bit with 10,000 rounds, meaning it keeps routing performance high while deploying low energy. This is particularly important for energy constrained battery-powered IoT nodes. Trust-based Routing is much more energy inefficient with J/bit consumption averages over 0.017 J/bit in all rounds. BBTR does a bit better at around 0.015 J/bit. ROUTENET was more in line with G-TrustChain, but still higher at around ~0.0132 J/bit on average. The reduced energy overhead in G-TrustChain is due to GNN guidance on route optimization and it is avoidance of excessive communication overhead from Blockchain trust validations.

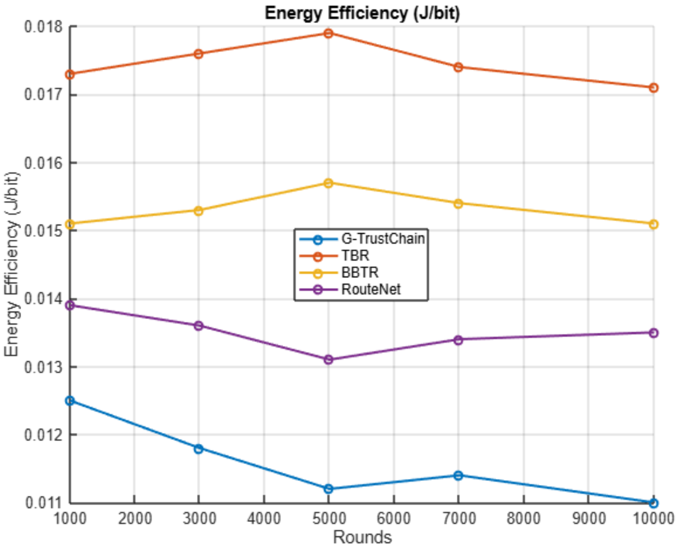

Figure 4. Energy consumption v/s number of rounds

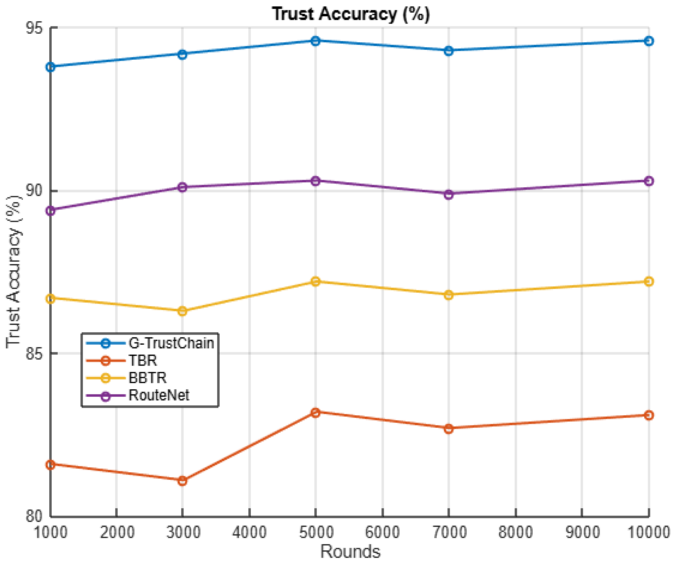

Figure 5. Trust accuracy (%) v/s number of rounds

4.3.4 Trust accuracy and attack detection

The G-TrustChain framework achieved 94.6% trust classification accuracy, outperforming average accuracies of around 83% for traditional threshold-based trust systems. Attack detection rates were also consistently high, achieving a 91.2% true positive rate for blackhole attacks, over 88% for Sybil attacks, and a comparable detection rate for wormhole type scenarios. The GNN's pattern recognition working in conjunction with the validation of the Blockchain appear to be effective approaches in the detection, and prevention concern as shown in Table 1.

Figure 5 shows the trust accuracy comparison of G-TrustChain's framework with other existing frameworks. G-TrustChain keeps impressive Trust Accuracy above 94% with the highest recorded Trust Accuracy of 94.6% at 10,000 rounds, showing its consistency of identifying trustworthy and malicious nodes. Since G-TrustChain decides if a node is trustworthy, based on learning from three different types of features with the GNN (latency, energy, historical trust score), we see G-TrustChain outperform in its classification accuracy. Trust-based Routing varies with a TA value as low as 81.1%, demonstrating Trust-based Routing 's ineptness in accurately modeling trust in dynamic networks, while BBTR and ROUTENET, perform better taking TA values 90.3%, but both still lower than G-TrustChain. G-TrustChain has a higher TA, and this TA indicates the ability of the solution to adapt and operate robustly in real-time trust inference.

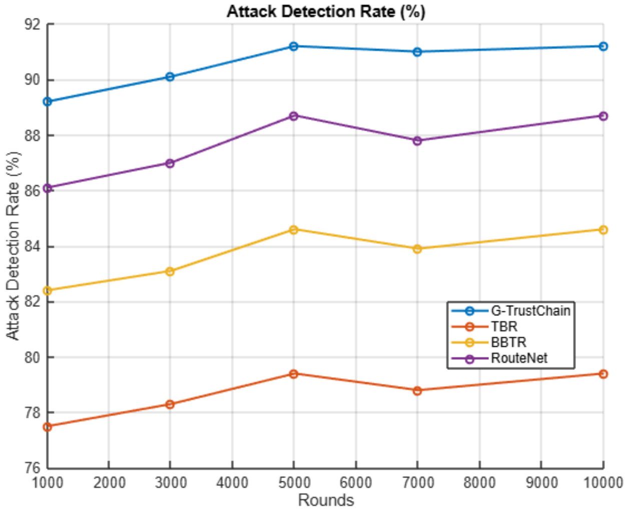

Figure 6. Attack detection rate (%) v/s number of rounds

Figure 6 shows the attack detection rate comparison of G-TrustChain's framework with other existing frameworks. The G-TrustChain’s ADR is the highest amongst the other frameworks compared to it, 91.2% at 10,000 rounds. This demonstrates the framework’s capacity to detect and act against adversarial actions effectively which is fundamental for secure routing in hostile settings. The detection rates increase to 89.2% and maintain this level after a while, when they stabilize above 80%, so the length has some effect, due to the cumulative knowledge of attacks in the GNN coupled with dwelling on past witness histories from trust logs in the Blockchain. Trust-based Routing has bottomed out around ADR detection rates as low as 77.5, while BBTR was unable to win 85%, off secure routing. ROUTENET achieves ADR detection rates of 88.7%, thanks to the GNN modeling, but does not have the block-chain verification of all time that G-TrustChain has.

4.3.5 Network lifetime

The G-TrustChain framework continues to maintain a greater alive node count across all tested rounds, showing its energy efficient and lightweight routing characteristics. Table 2 and Figure 7 show the network lifetime comparison of G-TrustChain's framework with other existing frameworks. Even at 1000 rounds, G-TrustChain maintains all nodes alive due to minimal overhead and less broadcast redundancy through GNN-guided path selection and trust based routing. After 10,000 rounds, G-TrustChain still has 92% of all nodes alive, thus demonstrating significant longevity in the network. The Trust-based Routing and BBTR frameworks begin to lose nodes earlier than G-TrustChain. By 3000 rounds, they have dropped to 93 alive nodes and then decreases to 75 alive nodes at 10,000 rounds post 10,000 rounds. The loss of alive nodes from Trust-based Routing can be attributed to the overhead of trust score recalculation, high communication cost of scaling trust values, and not effectively adapting its routing based on detected changes in a dynamic environment. BBTR fared better than Trust-based Routing due to its Blockchain reputation based approach However, overall BBTR suffered from heavier overall energy consumption than G-TrustChain.

Table 2. Performance evaluation and comparison at various rounds of simulations

Rounds	Framework	PDR (%)	Delay (ms)	Energy Efficiency (J/bit)	Trust Accuracy (%)	ADR (%)	Alive Nodes
1000	G-TrustChain	**95.1**	**84**	**0.0125**	**93.8**	**89.2**	**100**
	Trust-based Routing [1]	89.3	114	0.0173	81.6	77.5	98
	BBTR [2]	90.5	107	0.0151	86.7	82.4	99
	ROUTENET [3]	91.7	95	0.0139	89.4	86.1	99
3000	G-TrustChain	**95.6**	**82**	**0.0118**	**94.2**	**90.1**	**99**
	Trust-based Routing	88.5	118	0.0176	81.1	78.3	93
	BBTR	90.1	108	0.0153	86.3	83.1	94
	ROUTENET	92.1	94	0.0136	90.1	87.0	96
5000	G-TrustChain	**94.9**	**81**	**0.0112**	**94.6**	**91.2**	**98**
	Trust-based Routing	87.9	119	0.0179	83.2	79.4	88
	BBTR	89.6	106	0.0157	87.2	84.6	90
	ROUTENET	91.5	93	0.0131	90.3	88.7	94
7000	G-TrustChain	**94.3**	**83**	**0.0114**	**94.3**	**91.0**	**96**
	Trust-based Routing	88.1	115	0.0174	82.7	78.8	82
	BBTR	90.2	105	0.0154	86.8	83.9	90
	ROUTENET	91.8	94	0.0134	89.9	87.8	91
10000	G-TrustChain	**94.2**	**82**	**0.0110**	**94.6**	**91.2**	**92**
	Trust-based Routing	89.5	110	0.0171	83.1	79.4	75
	BBTR	90.8	105	0.0151	87.2	84.6	78
	ROUTENET	91.6	98	0.0135	90.3	88.7	85

The ROUTENET framework also demonstrates stable energy handling, with 85 nodes alive at 10,000 rounds. While the framework benefit from graph learning, it does not have a lightweight consensus mechanism and optimized trust routing, which led to lower performance for node lifespan than G-TrustChain.

The alive node metric illustrates that G-TrustChain not only increases security and trustworthiness of routing but it also greatly improves network sustainability, which is an important requirement for large scale IoT systems and networks. To establish the meaningfulness of the observed results, a two-tailed t-test was completed at the 95% confidence level comparing PDR and trust accuracy against baseline measures. For PDR and trust accuracy both, p-values were lower than 0.01, demonstrating that the observed improvements are statistically significant. So, G-TrustChain provides a resilient energy efficient routing protocol that outperforms the traditional and most recent secure routing systems in IoT networks. The combination of GNNs and Blockchain-based trust verification produce insider measurable improvements in trust accuracy, legitimate packet reliability, and resistance to adversaries.

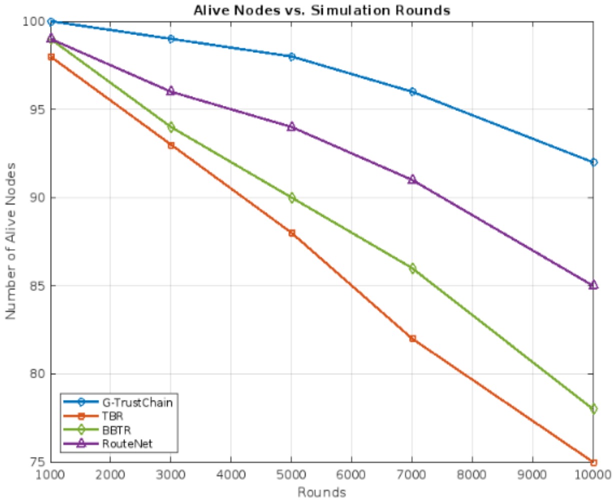

Figure 7. Alive nodes v/s number of rounds

G-TrustChain shows superior performance over TrustRank and BBTR, and SecureIoT-GNN across several key metrics such as PDR and EED. We attribute G-TrustChain's superior PDR (94-96%) not only to the fact that we can isolate malicious or low-trust nodes before making routing decisions through dynamically trusting our nodes, but also because TrustRank always assigns trust statically or probabilistically and therefore is slower to adapt to varying attack patterns, leading to sporadic packet drops along routes while contributing to the lower delivery rates in general. BBTR and SecureIoT-GNN improve upon TrustRank as they leverage blockchain-based validation and GNN inference, but they still share delays in update processes for trust scores due to high or dense mobility in other words, networks with constant changes of connections or nodes converging or departing; while leading to lower trust and PDR respectively, than G-TrustChain.

5. CONCLUSIONS

This paper presented G-TrustChain, a new hybrid framework that fuses GNNs with Blockchain-led trust scoring to enable secure and efficient routing in IoT networks. In this study, GNNs effectively learned topological and trust-based features for dynamic routing decisions while incorporating a lightweight Blockchain ledger to preserve immutable and tamperproof trust records. Results indicated that G-TrustChain outperformed established performance metrics as compared to benchmark frameworks such as Trust-based Routing, BBTR, and ROUTENET. The results for G-TrustChain achieved a higher packet delivery ratio of up to 95.6%, lower energy consumption of 0.0110 J/bit, higher trust accuracy above 94%, and higher attack detection rates greater than 91%, while sustaining low latency and high survivability greater than 95.4% over 10,000 rounds.

Based on the research and development in this paper, there are many pathways to develop G-TrustChain further. A great first next step can build upon federated learning to train GNNs in a distributed fashion across edge nodes to improve scalability and privacy. Additionally, adaptive Blockchain processes such as Layer-2 solutions will also suit to improve low-latency and reduce computation and space over time. Finally, expansion towards supporting heterogeneous IoT contexts, such as mobile or UAVs devices is also an important next step. Incorporating real-world testbed validations and expanding support for zero-trust architectures would help to further validate G-TrustChain's viability in practice.

REFERENCES

[1] Sennan, S., Somula, R., Kumar, R.L., Srinivasan, P., Jayanthi, M.A. (2021). Trust-aware routing framework for Internet of Things. International Journal of Knowledge and Systems Science, 12(1): 48-59. https://doi.org/10.4018/IJKSS.2021010104

[2] Dai, H.N., Zheng, Z.B., Zhang, Y. (2019). Blockchain for Internet of Things: A survey. arXiv preprint arXiv: 1906.00245. https://doi.org/10.48550/arXiv.1906.00245

[3] Raj, R., Ghosh, M. (2023). A Lightweight Blockchain Framework for secure transaction in resource constrained IoT devices. In 2023 5th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, pp. 1-7. https://doi.org/10.1109/RAIT57693.2023.10126898

[4] Bhutta, M.N.M., Khwaja, A.A., Nadeem, A., Ahmad, H.F., Khan, M.K., Hanif, M.A., Song, H., Alshamari, M., Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. IEEE Access, 9: 61048-61073. https://doi.org/10.1109/ACCESS.2021.3072849

[5] Swamy, S.N., Shivanarayanamurthy, P., Purohit, G., Kota, S.R. (2022). An edge computing-assisted Internet of Things-based secure smart home. In Proceedings of International Conference on Computational Intelligence and Data Engineering. Lecture Notes on Data Engineering and Communications Technologies, pp. 159-173. https://doi.org/10.1007/978-981-16-7182-1_14

[6] Shan, Y.X., Yang, J.L., Gao, Y.X. (2024). GL-GNN: Graph learning via the network of graphs. Knowledge-Based Systems, 299: 112107. https://doi.org/10.1016/j.knosys.2024.112107

[7] Rui, K.K., Pan, H.Z., Shu, S. (2023). Secure routing in the Internet of Things (IoT) with intrusion detection capability based on software-defined networking (SDN) and Machine Learning techniques. Scientific Reports, 13: 18003. https://doi.org/10.1038/s41598-023-44764-6

[8] Luo, T.X., Wang, J., Yan, Z., Gelenbe, E. (2025). Graph neural networks for trust evaluation: Criteria, state-of-the-art, and future directions. IEEE Network, 39(4): 37-46. https://doi.org/10.1109/MNET.2025.3551068

[9] Al-Rakhami, M.S., Al-Mashari, M. (2021). A blockchain-based trust model for the Internet of Things

supply chain management. Sensors, 21(5): 1759. https://doi.org/10.3390/s21051759

[10] Shahin, R., Sabri, K.E. (2022). A secure IoT framework based on blockchain and machine learning. International Journal of Computing and Digital Systems, 11(1): 671-683. https://doi.org/10.12785/ijcds/110154

[11] Wu, C.H., Wu, F.Z., Lyu, L., Qi, T., Huang, Y.F., Xie, X. (2022). A federated graph neural network framework for privacy-preserving personalization. Nature Communications, 13: 3091. https://doi.org/10.1038/s41467-022-30714-9

[12] Biswas, K., Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. In 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, NSW, Australia, pp. 1392-1393. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

[13] Altaf, T., Wang, X., Ni, W., Yu, G.S., Liu, R.P., Braun, R. (2024). GNN-based network traffic analysis for the detection of sequential attacks in IoT. Electronics, 13(12): 2274. https://doi.org/10.3390/electronics13122274

[14] Uludag, M.K., Karakus, M., Guler, E., Uludag, S. (2024). Adaptive mitigation of blackhole attacks in blockchain-enhanced software defined networks. In 2024 IEEE International Performance, Computing, and Communications Conference (IPCCC). Orlando, FL, USA, pp. 1-8. https://doi.org/10.1109/IPCCC59868.2024.10850069

[15] Arifeen, M.M., Mamun, A.A., Ahmed, T., Kaiser, M.S., Mahmud, M. (2020). A blockchain-based scheme for sybil attack detection in underwater wireless sensor networks. In Proceedings of International Conference on Trends in Computational and Cognitive Engineering. Advances in Intelligent Systems and Computing, pp. 467-476. https://doi.org/10.1007/978-981-33-4673-4_37

[16] Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A. (2021). Secure computation offloading in blockchain based IoT networks with deep reinforcement learning. IEEE Transactions on Network Science and Engineering, 8(4): 3192-3208. https://doi.org/10.1109/TNSE.2021.3106956

[17] Sun, H.L., Bi, X.F., Tu, Z.Y., Zhao, B.H., Zhang, K., Chu, D.H., Xu, X.F. (2025). Enhancing privacy-preserving knowledge graph embeddings with federated learning for IoT services. ACM Transactions on Internet Technology. https://doi.org/10.1145/3747351

[18] Sunitha, R., Chandrika, J., Pavithra, H.C. (2023). Machine learning techniques to combat security threats in social Internet of Things. International Journal of Research in Engineering, Science and Management, 6(3): 81-93.

[19] H D, K., G K, S., M, C., Dhananjaya, S., K P, S., Jairam, B.G., R, S. (2025). Privacy-preserving IoT framework with Federated Learning and lightweight NLP integration. Journal Européen des Systèmes Automatisés, 58(5): 953-961. https://doi.org/10.18280/jesa.580509

[20] K, M., Jayaram, K., T, S., Satyanarayana, H.T., S, S., D, S.S., V, L. (2025). Energy-efficient IoT network routing model based on multi-layer clustering and deep learning. Journal Européen des Systèmes Automatisés, 58(5): 1031-1039. https://doi.org/10.18280/jesa.580516

[21] Boulkamh, C., Derdouri, L., Bourouis, A. (2025). Quantum Cognitive Internet of Things framework for energy consumption prediction and optimization in smart home. Journal Européen des Systèmes Automatisés, 58(5): 1065-1078. https://doi.org/10.18280/jesa.580519

[22] Kruthik, J.T., Ramakrishnan, K., Sunitha, R., Prasad Honnavalli, B. (2021). Security model for Internet of Things based on blockchain. In Innovative Data Communication Technologies and Application. Lecture Notes on Data Engineering and Communications Technologies, pp. 543-557. https://doi.org/10.1007/978-981-15-9651-3_45

[23] Sunitha, R., Chandrika, J. (2021). Malevolent node detection based on network parameters mining in wireless sensor networks. International Journal of Digital Crime and Forensics, 13(5): 130-144. https://doi.org/10.4018/IJDCF.20210901.oa8

[24] Kumar, A.P., R, S., M, C., Dhananjaya, S., N, K.M., G, N. (2024). An energy-efficient and secure WSN routing protocol using Bayesian networks and elitist genetic algorithms. Journal Européen des Systèmes Automatisés, 57(6): 1547-1555. https://doi.org/10.18280/jesa.570601

[25] Al Hwaitat, A.K., Almaiah, M.A., Ali, A., Shishakly, R., Lutfi, A., Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. Electronics, 12(17): 3618. https://doi.org/10.3390/electronics12173618

[26] Guo, Y.M., Wang, Y., Khan, F., Al-Atawi, A.A., Al Abdulwahid, A., Lee, Y., Marapelli, B. (2023). Traffic management in IoT backbone networks using GNN and MAB with SDN orchestration. Sensors, 23(16): 7091. https://doi.org/10.3390/s23167091

[27] Ullah, F., Salam, A., Amin, F., Khan, I.A., Ahmed, J., Zaib, S.A. (2024). Deep trust: A novel framework for dynamic trust and reputation management in the Internet of Things (IoT)-based networks. IEEE Access, 12: 87407-87419. https://doi.org/10.1109/ACCESS.2024.3409273

[28] Wang, C.S., Tan, X.C., Yao, C.Y., Gu, F., Shi, F.L., Cao, H.Q. (2022). Trusted blockchain-driven IoT security consensus mechanism. Sustainability, 14(9): 5200. https://doi.org/10.3390/su14095200

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

[30] Xie, Z.Y., Huang, Y.H., Fang, G.Q., Ren, H.X., Fang, S.Y., Chen, Y.R. (2018). RouteNet: Routability prediction for mixed-size designs using convolutional neural network. In 2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Diego, California USA, pp. 1-8. https://doi.org/10.1145/3240765.3240843