SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Entropy–Trust–Causality Driven Secure Routing Framework For Adversarial Network Environments Using Quantum Inspired Path Optimization And Digital Twin Validation In Practical Scenarios

Rahul Mahajan[1] and Srikant V. Sonekar[2]

[1]PGDT, Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur, Maharashtra, India.
[2]JD College of Engineering and Management, Nagpur, Maharashtra, India.
rahulmahajan3102@gmail.com[1], srikantsonekar@gmail.com[2]

Abstract: As communication infrastructure modernizes, including IoT, cyber-physical systems, and high-volume distributed systems, they continue to be targeted by advanced forms of attacks that impact how routing takes place, affect the integrity of trust relationships, and negatively influence network reliability. Therefore, there is an urgent need for secure routing paradigms that are adaptable, and analytically proven to work across changing topologies and stealthy malicious nodes, especially given the limitations of current routing paradigms to account for topology level changes, evolving patterns of malicious behavior, and propagation characteristics of malicious traffic. In addition, many of the existing secure routing frameworks do not include integrated validation frameworks that are able to trace causality of an attack and evaluate the resilience of a routing paradigm under controlled simulation of adversarial conditions. To meet this challenge, a multi-phase framework for secure routing in adversarial network environments is presented. The framework begins with AGEP-NET, the Adversarial Graph Entropy Profiling Network, that models network communication as time-dependent entropy-based graphs to determine abnormal interaction of nodes; the structure formed from the graph processing is used in MATPRS, the Multi-Agent Trust Propagation Reinforcement System, to allow routers to cooperatively use reinforcement learning to develop trust relationships. Following the development of the trust relationships, CATDM, the Causal Adversarial Traffic Decomposition Model, determines causal linkages of malicious traffic propagations. Then QSPOE, the Quantum Inspired Secure Path Optimization Engine, develops candidate routing paths based upon the probability of each path being explored. Finally, DTANS, the Digital Twin Adversarial Network Simulator, tests the resilience of routing paradigms against different types of attack. Overall, the proposed framework enhances the ability to detect adversaries, increases routing reliability and improves overall network resiliency. These improvements provide a solid foundation for the development of future secure routing paradigms for Next Generation distributed systems and adversarial communication environments.

Keywords: Secure Routing, Adversarial Network Environments, Trust Propagation Learning, Quantum Inspired Optimization, Digital Twin Network Security, Analysis.

1. Introduction

Modern communication networks are increasingly deployed in environments in which adversaries can [1, 2, 3] manipulate routing infrastructure with sophistication and persistence to support real-time deployment. Many distributed systems, including Internet-of-Things (IoT) ecosystems, cyber-physical infrastructures, industrial automation networks, and edge-cloud architectures rely upon dynamic routing protocols to ensure reliable communication between diverse devices. Adversaries frequently take advantage of vulnerabilities in routing protocols in order to launch attacks such as manipulating wormholes, injecting Sybil identities, absorbing blackhole packets, and poisoning routing tables. Such adversarial manipulations distort perceptions of network topology, degrade the reliability of packet delivery, and ultimately impact the availability and integrity of communications

systems. Prior approaches to addressing the challenges posed by routing attacks, particularly those involving exponentially [4, 5, 6] elaborate and secure routing schemes, have utilized signature-based intrusion detection mechanisms, rule-based anomaly detection, and static trust evaluation models. Although prior approaches offered some degree of protection against routing attacks, they were limited in their ability to capture the structural dynamics of network interaction and focused primarily on packet-level or node-level attacks. Today's most sophisticated attacks leverage topological vulnerabilities rather than the isolation of packet anomalies. Therefore, while many routing security approaches utilize traffic statistical analysis and/or predefined behavioral threshold models to determine whether a given node exhibits anomalous behavior, they often fail to detect coordinated/distributed attack patterns. Moreover, many prior routing security approaches assumed relatively stable network conditions; however, today's distributed networks exhibit dynamic topology changes, heterogeneity in terms of node capabilities, and continually evolving communication patterns.

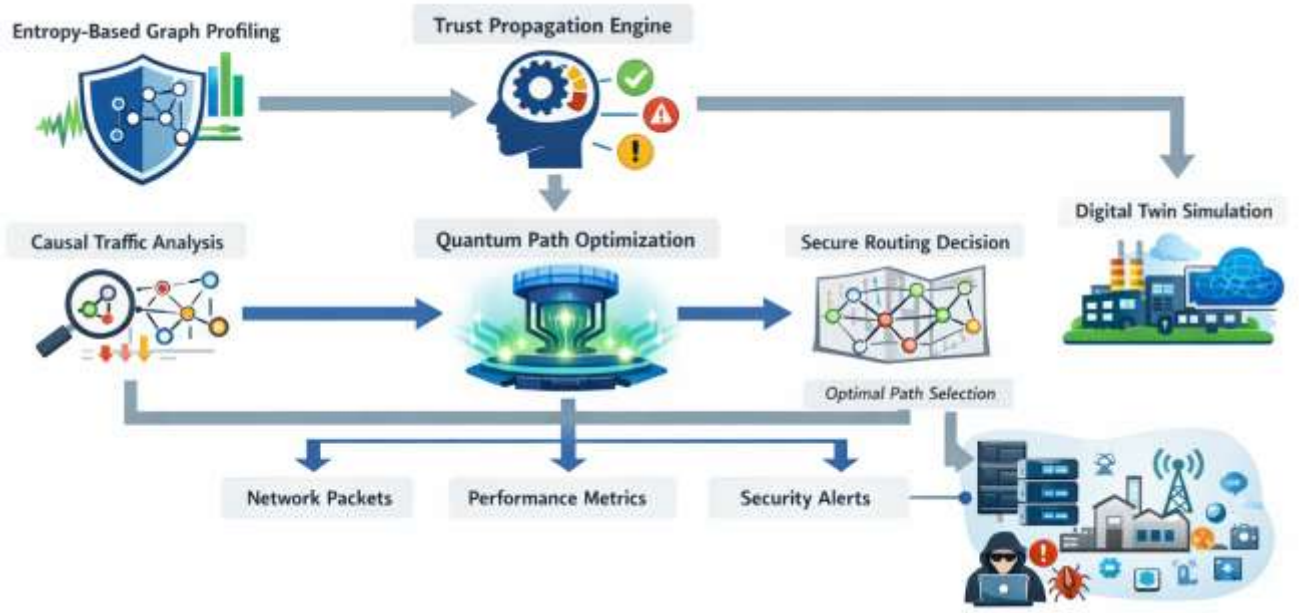

Figure 1. Model's Integrated Architectural Analysis

Another shortcoming observed in the prior literature is the lack of a fully integrated pipeline capable of identifying all phases of the adversarial behavior lifecycle in a network process. There exist several models that focus primarily on identifying anomalous nodes [10, 11, 12]; however, few models have investigated how malicious traffic propagates along routing paths or how compromised nodes influence neighbor routing decision-making. Without understanding causality, most mitigation strategies tend to be reactive versus preventative. Additionally, optimization algorithms employed in the determination of secure routing options typically emphasize routing metrics (e.g., shortest path, energy efficiency), without accounting for the adverse risks associated with malicious intermediate nodes. As a consequence [13, 14, 15], routing options determined by such algorithms may contain nodes that are part of hidden attack chains. Advances in artificial intelligence and network analytics have provided opportunities to develop multi-phase intelligent routing architectures to overcome the limitations identified above. Graph-based learning models enable the representation of complex network interactions, reinforcement learning enables adaptive trust modeling among cooperative nodes, and causal inference techniques provide insight into the propagation mechanisms of adversarial traffics. Quantum Inspired optimization approaches also have shown significant potential in resolving complex combinatorial search problems such as determining secure routing options under multiple security constraints. When combined with digital twin simulation frameworks capable of simulating real-world network conditions, these technologies have enabled the creation of powerful platforms for developing robust and verifiable secure routing models.

This paper presents an integrated analytical framework that enhances routing security in adversary impacted network environments. The proposed framework as per figure 1, employs entropy-based graph profiling to identify structural anomalies in communication patterns and utilizes trust propagation learning among distributed routing agents to model the evolving levels of trust amongst routing agents in a distributed network environment. A causal traffic decomposition layer is used to analyze the propagation dependency relationships in order to expose the sources of the attack and the paths influenced by the attack. Using a quantum-inspired optimization engine, the proposed framework generates secure routing decisions by evaluating candidate paths under multiple types of adversarial risk constraints. Finally, a digital twin network simulator provides controlled experimental validation

by simulating realistic attack scenarios and measuring the routing resiliency under dynamic conditions. By employing an integrated analytical architecture that identifies adversarial nodes early, provides adaptive trust learning across distributed routers, and includes causal reasoning to understand attack propagation mechanisms, the proposed framework fills critical gaps in the current secure routing research process. Additionally, the inclusion of advanced optimization and simulation methodologies in the proposed framework ensure that the routing decisions made will continue to be resilient against evolving network threats. Collectively, the contributions of the advancements presented in this paper contribute to the continued development of intelligent and robust routing infrastructures required to support Next Generation distributed communication systems.

Motivation and Contributions

As the number of large scale distributed networks grows, the difficulty of securing routing architectures is growing with them. Large scale communication systems are made up of many interconnected devices running on different hardware and software platforms (IoT sensor, edge node, gateway to the cloud, and mobile devices and applications). Routing protocols must be able to function efficiently, and deal with the increasing numbers of new security threats appearing. Malicious actors are now able to utilize vulnerabilities in routing algorithms to alter network topologies, reroute packets through intermediary malicious actors, or block traffic flow across important nodes. Many times malicious actors can execute their attacks without being detected as their attack mimics normal routing behaviors but slightly alters the way the data flows across the network. Therefore, current routing architectures have no effective means to defend against continuous evolving coordinated malicious strategies. Thus, the motivation for this work is to develop a routing security architecture that will be able to perform analysis at various structural levels of network behavior, while also being able to make adaptive decision making. Unlike traditional approaches to routing security that rely on static rules or standalone anomaly detection methods, the proposed solution utilizes a combination of graph based analytics, reinforcement learning, causal inference, and probabilistic optimization to develop a comprehensive and adaptive security pipeline. This allows the routing system to identify structural abnormalities, establish trust relationships among nodes, analyze the propagation characteristics of malicious traffic, and choose secure routing paths that take into account potential malicious actor risk. Therefore, the research aims to provide a scalable solution to address both detection and mitigation of malicious activity in a dynamic network environment.

This research's major contribution is developing a multi-stage intelligent routing framework that converts raw network data into routing security decisions through a series of analytical models. The first contribution develops an entropy based graph profiling method that represents the structural communication patterns of network nodes and identifies anomalies associated with malicious actor interaction. Based on the graph representation, a multi agent trust propagation learning method is developed so that cooperative routers can use reinforcement driven learning to establish reliable relationships amongst each other. The third contribution develops a causal method for decomposing adversarial traffic, which allows the routing infrastructure to trace the chain of events associated with malicious traffic and determine the source of malicious activity within a complex traffic flow. Finally, to ensure that routing decisions are robust against identified threats, a Quantum Inspired Secure Path Optimization Engine is developed to find optimal routes using probabilistic state exploration and incorporate both performance and security constraints into the evaluation. The final contribution combines all of the previously described analytic components into a Digital Twin Network Simulation Environment that can simulate realistic scenarios involving adversarial actors and used for experimental Validation In Process. Overall, the above described architecture provides a complete pipeline for performing analysis on routing security related to adversarial actors, from anomaly detection and establishing trust relationships to performing causal analysis, optimization, and evaluating the results through simulations. Therefore, the proposed architecture advances the state of the art for secure routing by providing a holistic methodology to improve the resilience of networks, improve the reliability of packet delivery, and mitigate the disruption caused by malicious actors in today's large scale distributed communication systems.

2. Review of Existing Models used for Analysis

The increase in the number of intelligent communication infrastructures has increased the demand for robust security solutions that can be used in hostile environments for communications. Many current distributed systems (IoT, WSN, CPN, ITS) use self-configuring routing and data transmission protocols. These systems still suffer from advanced attacks like routing manipulation, traffic injection, stealth intrusion, and trust exploitation. To combat this, early research has concentrated on developing detection and monitoring frameworks to detect malicious behavior of transmitted traffic within distributed networks. For example, Verma et al. developed a framework to detect adversarial attacks against IoT networks, which utilizes behavioral anomaly detection/monitoring to identify malicious communication patterns [1]. The authors showed that monitoring frameworks can successfully identify

unusual traffic flow; however, the authors' work primarily focused on identifying intrusions and not the larger problem of how to make routing decisions securely. Based on the need for more resilient routing methods, Mahajan and Sonekar developed a secure routing model utilizing both CAFR-Net and EPM-Core architectures to reduce adversarial influence on routing decisions [2]. Their work highlighted the combination of adversarial defensive mechanisms with routing optimizations; however, their model used limited feature representation and did not include dynamic behavioral trust learning nor causal traffic propagation analysis. Advancements in adversarial learning and deep neural inference also broadened the applicability of security frameworks intended to protect hostile network environments. Li et al. created the FSAT framework to combine adversarial training techniques with secure CNN inference for improving robustness in resource constrained environments [3]. They demonstrated that adversarial training could improve model robustness, but the primary focus of the work was on improving inference rather than on securing routing architecture. Concurrently, Kumar proposed a genetic algorithm based secure hybrid routing technique for IoT networks that utilized evolutionary optimization to find efficient routing paths under security constraints [4]. Evolutionary optimization provided better routing efficiency; however, the method failed to capture the complexities of traffic propagation that exist in dynamic adversarial environments. Deep neural architectures were then incorporated into security frameworks by Aldaej et al. who proposed a DNN-based secure healthcare communication framework to protect the transmission of sensitive medical information [5]. The work demonstrated strong predictive capability; however, it was specific to an application and did not address more general routing security concerns in large-scale networks. Following Aldaej et al.'s work, subsequent studies transitioned to designing optimized machine learning models to detect adversarial networks. Barik et al. proposed an adversarial attack detection framework that utilized optimized weighted conditional stepwise adversarial networks to improve detection accuracy by adaptively optimizing weights throughout training [6] process.

Table 1. Model's Empirical Review Analysis

Reference	Method	Main Objectives	Findings	Limitations
[1]	Secure Adversarial Attack Detector Framework for IoT Intrusion Monitoring	Develop a framework for detecting adversarial intrusions in IoT communication networks using behavioral monitoring and anomaly detection mechanisms.	The framework improved intrusion detection capability in IoT traffic monitoring and demonstrated high detection accuracy for abnormal communication flows.	Focused primarily on intrusion detection; routing security and adaptive mitigation strategies were not addressed.
[2]	CAFR-Net and EPM-Core Secure Routing Model	Design a secure routing mechanism capable of identifying adversarial nodes and improving routing reliability within hostile network environments.	The model improved routing security and network reliability by integrating adversarial node identification with path optimization.	Limited feature representation and lack of dynamic trust learning and causal traffic modeling.
[3]	FSAT Secure CNN Inference with Adversarial Training	Improve secure neural network inference in resource-constrained environments through adversarial training and optimized CNN inference pipelines.	Demonstrated improved robustness of neural inference models against adversarial perturbations while maintaining computational efficiency.	Primarily focused on secure model inference rather than routing infrastructure security.
[4]	Genetic Algorithm-Based Secure Hybrid Routing Technique	Develop an optimization-based routing approach for IoT networks using genetic algorithms to improve routing efficiency and security.	Achieved improved routing efficiency and reduced packet loss under adversarial scenarios through evolutionary path optimization.	Evolutionary search increases computational complexity and lacks real-time adaptability to dynamic attacks.

[5]	Deep Neural Network-Based Secure Healthcare Communication Framework	Protect sensitive healthcare communication systems using deep neural network models for secure data transmission.	Demonstrated strong predictive capability for detecting malicious data transmission in healthcare networks.	Application-specific design limits applicability to broader network routing scenarios.
[6]	Optimized Weighted Conditional Stepwise Adversarial Network	Improve adversarial attack detection through optimized conditional adversarial learning strategies.	Enhanced detection accuracy of adversarial attacks by dynamically adjusting feature weights during training.	Focuses on attack detection rather than integrated routing security mechanisms.
[7]	Transformer-Based Adversarial Network for Steganography	Develop a transformer architecture capable of detecting adversarial perturbations in steganographic data.	Transformer-based architecture improved feature extraction and robustness against adversarial perturbations.	Application domain restricted to steganography rather than network routing security.
[8]	GAN-Assisted Power Management Framework	Use generative adversarial networks to optimize power management under adversarial operational conditions.	Demonstrated improved optimization of power consumption and system stability using adversarial learning.	Framework targets energy management rather than routing or network security infrastructure.
[9]	Blockchain-Enabled GNN Framework for Secure Routing	Integrate blockchain verification with graph neural networks to enhance routing security in IoT networks.	Improved trust verification and decentralized routing security using blockchain-supported trust evaluation.	Blockchain overhead introduces latency and computational cost for large-scale networks.
[10]	GAN-Based Robust Steganalysis Framework	Improve robustness of steganalysis systems in adversarial environments using generative adversarial learning.	Enhanced robustness of steganalysis detection models under adversarial manipulation scenarios.	Application limited to media steganalysis rather than network routing or infrastructure security.
[11]	Data-as-Infrastructure Secure Localization Framework	Develop a data-centric architecture for secure vehicle localization under adversarial interference conditions.	Improved localization reliability in intelligent transportation systems despite adversarial signal disruptions.	Framework focused on localization rather than secure routing or traffic propagation modeling.
[12]	FlexClave Trusted Execution Environment Framework	Design a secure execution environment for protecting sensitive computations in distributed systems.	Provided enhanced hardware-level security and isolation for executing critical network functions.	Focuses on secure execution rather than routing decision intelligence.
[13]	Energy-Efficient Secure Routing for Heterogeneous IoT Networks	Develop routing protocols balancing energy efficiency and security for heterogeneous IoT networks.	Demonstrated improved energy efficiency and reduced network overhead in secure routing operations.	Limited adversarial modeling and lacks advanced attack propagation detection mechanisms.
[14]	Cross-Layer Secure Semantic	Introduce GAN-based semantic noise	Improved resilience of semantic	Focuses on communication

	Communication Framework	modeling to improve secure communication reliability.	communication systems against adversarial interference.	robustness rather than routing optimization or network security architecture.
[15]	Adversarial Neural Network Training for Brain Communication	Improve robustness of neural communication systems through adversarial neural training strategies.	Enhanced robustness and reliability of brain-to-brain communication networks under adversarial disturbances.	Domain-specific application limits generalization to traditional network routing environments.
[16]	GNN-TASR Trust-Aware Secure Routing for LEO Satellite Networks	Develop a graph neural network-based routing model for secure communication in satellite networks.	Demonstrated improved trust-aware routing performance and network reliability in satellite communication systems.	Requires extensive graph training data and may struggle with rapidly changing network topologies.
[17]	NASim-Based Adversarial Pentest Environment	Create a simulation environment for evaluating penetration testing and defense strategies in adversarial networks.	Enabled realistic adversarial testing and defense strategy evaluation through simulation-based environments.	Simulation-focused framework without routing optimization or deployment-level integration.
[18]	TrMLGAN Transmission Multi-Loss GAN Framework	Improve signal restoration and transmission quality using multi-loss adversarial learning architecture.	Enhanced transmission quality and noise robustness in image communication systems.	Primarily image communication focused rather than network routing security.
[19]	On-Demand Fault-Tolerant Routing Strategy	Develop a routing protocol capable of maintaining communication reliability during failures in key distribution networks.	Improved reliability and fault tolerance in secure communication networks.	Limited adversarial threat modeling and absence of intelligent attack detection mechanisms.
[20]	Semi-Supervised GAN Framework for Pansharpening	Improve remote sensing image fusion quality using semi-supervised generative adversarial networks.	Enhanced feature reconstruction accuracy in image processing tasks.	Not directly applicable to secure network routing frameworks.
[21]	Secure Opportunistic Routing Framework	Develop opportunistic routing protocols for dynamic networks with improved security and efficiency.	Improved routing efficiency and sustainability in opportunistic communication environments.	Limited trust management and adversarial behavior detection capabilities.
[22]	GAN-Based Travel Time Reliability Prediction	Apply generative adversarial networks to predict transportation network reliability.	Demonstrated improved prediction accuracy for large-scale transportation network performance.	Focused on transportation analytics rather than communication routing security.
[23]	Geographic Webcasting Secure Routing Protocol	Introduce a geographic webcasting protocol for secure data routing in	Improved secure broadcast efficiency	Lacks advanced adversarial detection

		wireless sensor networks.	and geographic routing reliability.	and trust propagation capabilities.
[24]	Neural Network-Adaptive Secure Control Framework	Protect cyber-physical systems from adversarial attacks using adaptive neural control mechanisms.	Demonstrated strong resilience of nonlinear control systems against adversarial manipulation.	Focuses on system control rather than communication routing security.
[25]	DAG-Blockchain Trusted Routing Architecture	Develop a blockchain-based trusted routing mechanism using directed acyclic graph structures.	Improved trust management and data integrity within MANET-IoT routing environments.	Blockchain overhead introduces scalability concerns for large networks.
[26]	Secure Routing and Authentication Framework for Multimedia Sensor Networks	Provide privacy-preserving routing and authentication mechanisms for multimedia sensor communications.	Improved secure communication and authentication for multimedia sensor environments.	Limited adversarial attack modeling and routing intelligence.
[27]	Polymorphic Network Environment Framework	Introduce a theoretical architecture for dynamically adaptable network infrastructures.	Demonstrated flexible network architectures capable of adapting to changing operational environments.	Lacks implementation-level routing security mechanisms.
[28]	GAN and Genetic Algorithm Optimization Framework	Optimize environmental conditions using hybrid adversarial and evolutionary optimization strategies.	Demonstrated effective hybrid optimization combining GAN learning and evolutionary search.	Focused on infrastructure optimization rather than network routing security.
[29]	Secure Neural Network Inference Framework for Connected Vehicles	Enable secure neural inference operations in vehicular communication systems.	Improved security and reliability of neural inference tasks in connected vehicle environments.	Primarily addresses model inference security rather than routing architecture.
[30]	SafeLib Secure Network Function Outsourcing Framework	Provide a secure framework for outsourcing network functions to external infrastructures.	Demonstrated improved security and reliability for outsourced network services.	Does not directly address adversarial routing or trust-aware path optimization.

Iteratively, Next, as per table 1, A range of other researchers have also investigated routing techniques that are both secure and energy efficient. In particular, Thangavelu and Rajendran presented an energy-efficient routing method to be used for managing a heterogeneous IoT network, demonstrating the need to trade off energy consumption against security assurances when developing routing security protocols [13]. Subsequently, Ren and Li introduced a cross-layer secure semantic communication framework that uses GAN-based noise generation to increase the resilience of communication against adversarial interference [14]. Additionally, Ahmadi et al. developed neural communication systems that utilize adversarial training of neural networks to provide secure and robust brain-to-brain communication systems, illustrating the expanding applicability of adversarial learning across various communication paradigms [15]. A number of additional researchers have utilized graph-based routing methods to develop routing architectures that are capable of establishing trust-aware secure routing for different types of communication networks. Specifically, Naz et al. presented the GNN-TASR model that utilizes graph neural networks to determine the level of trust required to ensure secure routing of information packets in LEO satellite networks, and this demonstrates the ability of graph-based machine learning methods to model the complex interconnectivity that exists among distributed communication networks and their respective deployments [16]. Researchers have also examined a variety of techniques for evaluating and testing network security systems in adversarial testing environments. For example, Huo et al. developed a network pentest-defense adversarial environment using NASim, providing a platform to evaluate the effectiveness of simulated penetration testing

environments [17]. In related work involving adversarial modeling, Dwivedi and Chakraborty proposed the TrMLGAN framework for transmission multi-loss generative adversarial learning, illustrating how the use of adversarial learning architectures can help to improve the restoration of signals and increase the transmission reliability [18]. Wu et al. presented a novel on-demand fault-tolerant routing method for secure key distribution networks, illustrating the importance of fault tolerance in the design of secure routing [19]. In addition, Wang et al. proposed a semi-supervised GAN framework for pansharpening tasks, demonstrating the role that generative adversarial networks can play in enhancing the quality of data representations under uncertain conditions [20].

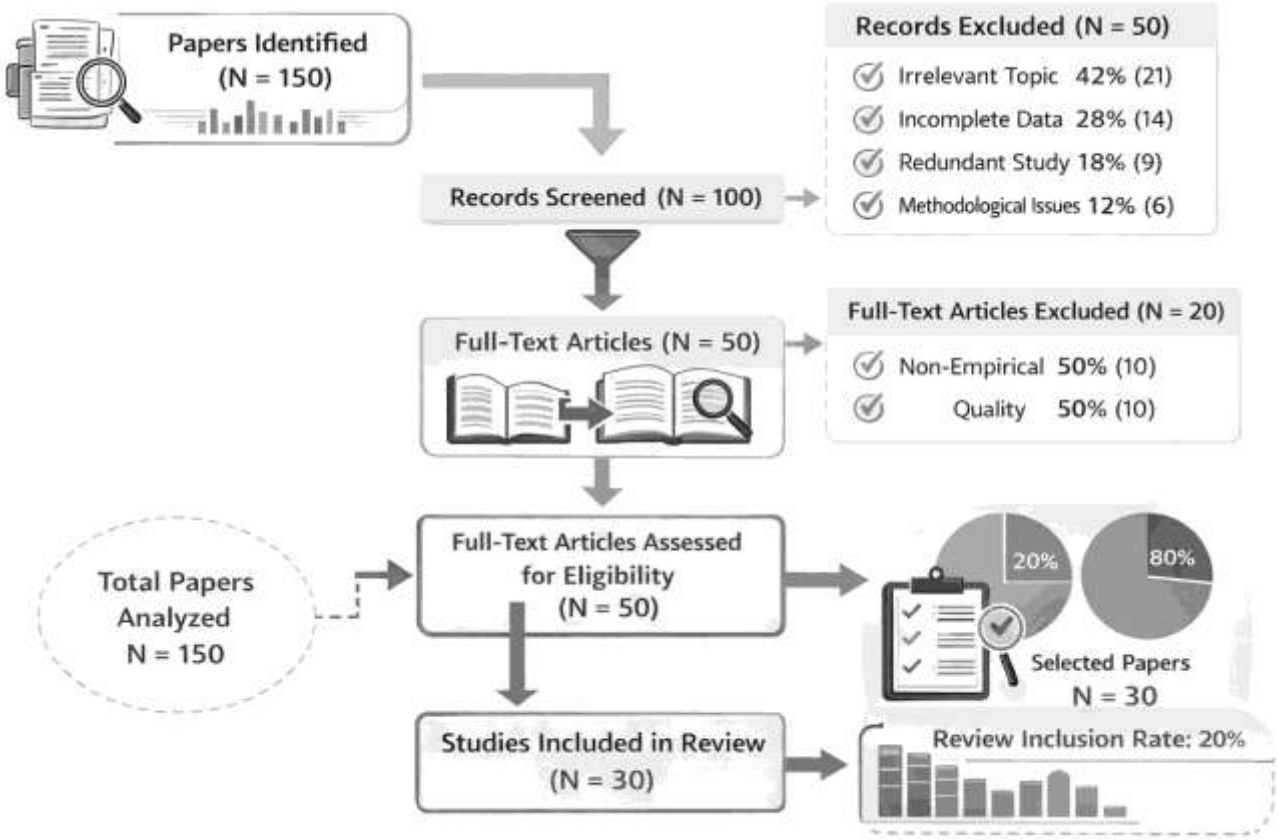

Figure 2. Methodological Review Selection Analysis

In addition to the previous advancements, a number of researchers have been investigating routing and communication architectures that are capable of securely communicating through dynamic network environments using opportunistic routing. For example, Khalil and Zeddini proposed a secure opportunistic network routing framework that was designed to improve the efficiency of communication while maintaining network sustainability [21]. Shao et al. utilized generative adversarial networks to predict the reliability of travel times in network-wide transportation systems, illustrating the flexibility of adversarial models in modeling large-scale dynamic systems [22]. Uma et al. proposed a geographic webcasting protocol for secure data routing in WSNs that improved geographic routing reliability while maintaining data confidentiality [23]. Zhao et al. further illustrated the application of neural network-adaptive secure control mechanisms to protect nonlinear CPSs from adversarial attacks [24]. In mobile ad hoc network environments, Ilakkiya and Rajaram introduced a DAG-blockchain routing structure that improves trust and reliability in MANET IoT systems [25]. Complementary to the above efforts, Baazeem presented a secure routing and authentication framework designed for multimedia sensor environments that provided enhanced privacy preservation and authentication mechanisms [26]. Later, Wu et al. introduced theoretical concepts regarding polymorphic network environments and proposed a flexible architectural framework that is capable of adapting to changing network conditions and adversarial threats [27]. Yu et al. proposed the combination of GANs and genetic algorithms to optimize environmental parameters in intelligent infrastructure systems, demonstrating the potential of hybrid optimization frameworks [28]. Yang et al. contributed to secure communication infrastructures by proposing a secure neural network inference framework for ICVs that enables secure computation in VCNs [29]. Finally, Marku et al. presented SafeLib, a comprehensive framework for

secure outsourcing of network functions, and highlighted the increasing importance of secure service orchestration in distributed network infrastructures [30].

Together, the research presented herein demonstrates considerable advancement in adversarial detection, trust modeling, neural security frameworks, and optimization-based routing strategies. However, there are still a number of limitations as per figure 2, evident in the current body of research process. Most notably, many of the frameworks that have been developed focus on either detecting adversarial attacks or optimizing routing in isolation, rather than developing a complete analytical pipeline that captures all aspects of the lifetime of adversarial network behaviours. Moreover, most routing security models do not incorporate causal traffic analysis, probabilistic path optimization, or simulation-driven validation within a single integrated architectural process. Therefore, the development of a comprehensive secure routing framework that integrates entropy-based structural analysis, adaptive trust propagation, causal traffic inference, quantum-inspired routing optimization, and digital twin validation is motivated by the identified gaps in the current state-of-the-art in order to provide a more holistic strategy for mitigating adversarial network threats while making reliable and efficient routing decisions in Next Generation distributed communication systems.

3. Proposed Model Design Analysis

The Integrated Secure Routing Framework (ISRF) is a Multi-Layer Analytical Pipeline that converts Raw Network Traffic Observations into Optimized Secure Routing Decisions under Adversarial Conditions. The ISRF Model combines entropy-driven graph analysis, reinforcement-based trust propagation, causal traffic inference, probabilistic routing optimization and digital twin validation in one Unified Mathematical Formulation Process. At each layer, the Routing Infrastructure produces Structured Intermediate Representations that serve as Inputs to Subsequent Layers to enable the Routing Infrastructure to incrementally improve its understanding of Network Reliability, Attack Propagation, and Path Security. The Design Assumption is a Distributed Communication Network represented as Dynamic Graph G = (V, E), where V represents the Set of Network Nodes and E represents Communication Links. Contextual Parameters for Each Edge include Bandwidth bij, Latency lij, Packet Loss Rate ρij, and Communication Frequency fij Sets. The Overall Objective of the ISRF Model is to Estimate Secure Routing Decisions that Maximize Network Reliability and Minimize Adversarial Influence over Routing Paths. Initially, As Per Figure 3, the First Analytical Stage Models the Network as Temporal Communication Graph and Computes Structural Uncertainty Using Entropy-Based Profiling Process. The Probability Distribution of Outgoing Communication Interactions Between Neighboring Nodes i and j Is Express Via Equation 1,

$$p_{ij}(t) = \frac{f_{ij}(t)}{\sum_{k \in N(i)} f_{ik}(t)} \dots (1)$$

Where fij (t) represents the Observed Communication Frequency Between Nodes i and j During Time Window t, and N(i) represents the Neighborhood Set of Node i in the Process. This Probabilistic Representation Captures Traffic Distribution Patterns That May Indicate Abnormal Routing Behaviors. Structural Uncertainty of Node Interactions Is Quantified Through a Temporal Entropy Measure Defined Via Equation 2,

$$H_i(t) = -\sum_{j \in N(i)} p_{ij}(t) \log\left(p_{ij}(t)\right) \dots (2)$$

Which Reflects the Variability of Communication Behavior Around Node i in Process. A Sudden Increase in Entropy Indicates Abnormal Traffic Diversification Often Associated with Adversarial Routing Manipulations.

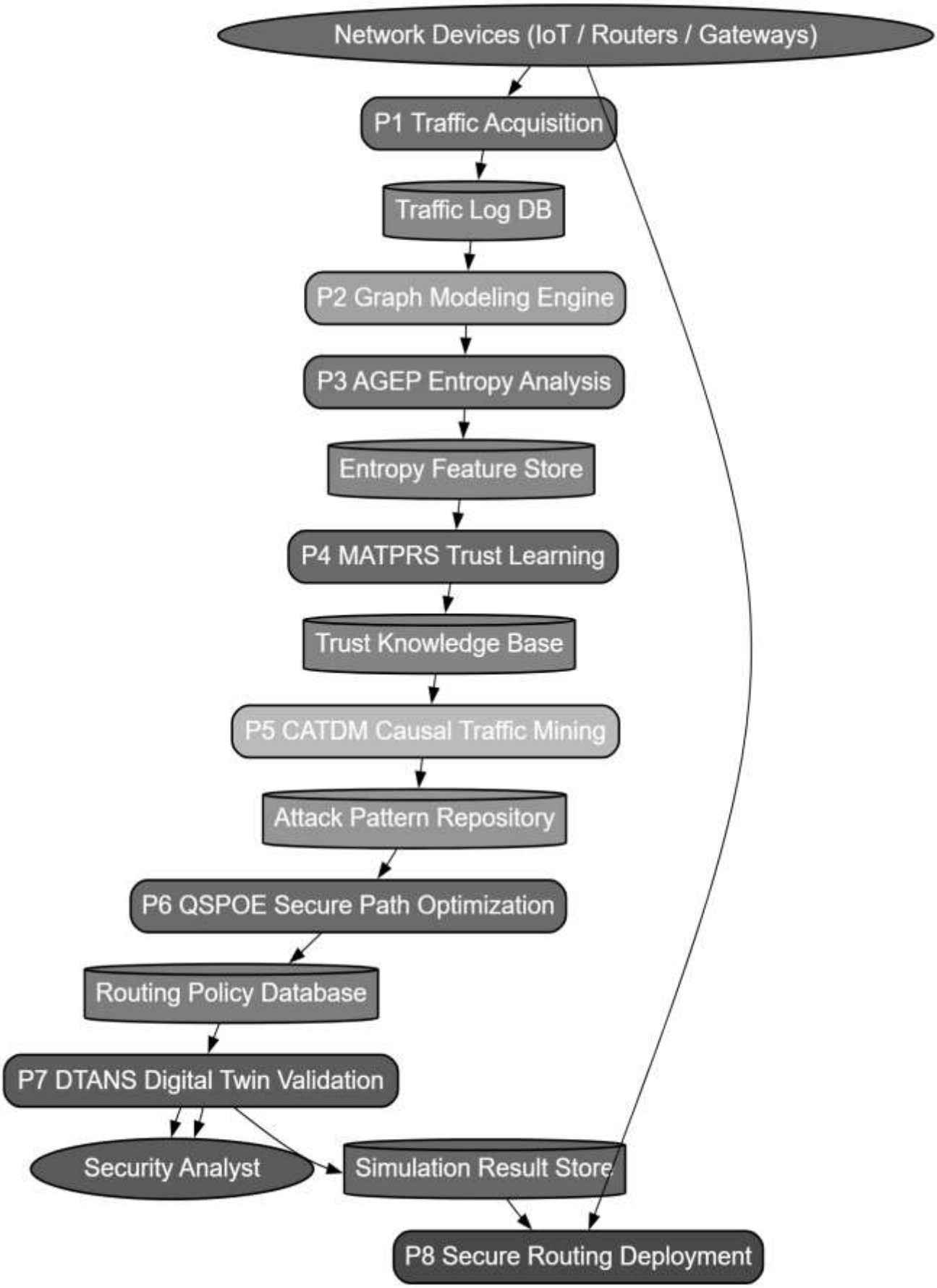

Figure 3. Model's Integrated Architectural Analysis

To Capture Temporal Evolution of Node Behavior, the Entropy Gradient Across Time Windows is Computed Via Equation 3,

$$\frac{dH_i(t)}{dt} = \lim_{\Delta t \to 0} \frac{H_i(t + \Delta t) - H_i(t)}{\Delta t} \dots (3)$$

Nodes with High Entropy Derivatives Indicate Rapidly Changing Communication Structures and Are Therefore Assigned Higher Adversarial Suspicion Scores. these Entropy-Derived Feature Vectors Form the Structural Input to the Trust Propagation Learning Model Process. The Second Stage Establishes Adaptive Trust Relationships Among Nodes Using a Reinforcement-Driven Trust Propagation Mechanism in Process. Each Node Maintains a Trust Score Ti (t) Reflecting Its Reliability Within the Network Deployments. Trust Values are Updated Through Iterative Learning Based on Interaction Outcomes and Entropy Signals Obtained from the Previous Stages. The Trust Update Process is Modeled Using a Reinforcement Reward Function Defined Via Equation 4,

$$T_i(t + 1) = T_i(t) + \alpha R_i(t) - \beta H_i(t) \dots (4)$$

Where Ri (t) represents Cooperative Reward Derived From Successful Packet Forwarding Behavior, While Hi (t) Penalizes Nodes Exhibiting Abnormal Communication Entropy. Iteratively, Next, As Per Figure 4, Parameters α and β Control the Influence of Cooperative Reinforcement and Anomaly Penalties Respectively for the Process. Trust Propagation Across Neighboring Nodes is Modeled Using a Weighted Diffusion Process Via Equation 5,

$$\frac{dT_i(t)}{dt} = \sum_{j \in N(i)} w_{ij} \left(T_j(t) - T_i(t)\right) \dots (5)$$

Where, wij represents Trust Influence Weights Between Nodes i and j in Process. This Differential Formulation Allows Reliable Nodes to Reinforce Trust Among Their Neighbors While Suppressing Adversarial Behavior Propagations. The Third Stage Performs Causal Traffic Decomposition to Identify Attack Propagation Pathways. Given Traffic Flows Between Nodes, Temporal Dependencies Among Routing Events are Represented Using Causal Influence Coefficients in Process. The Causal Influence from Node i to Node j is Estimated Using an Integral Formulation that Measures How Past Traffic Behavior Influences Future Packet Flows Via Equation 6,

$$C_{ij} = \int_0^T x_i(t) \frac{dx_j(t)}{dt} dt \dots (6)$$

Where, xi (t) and xj (t) represent Traffic Intensity Signals for Nodes i and j for this Process. A Large Value of CijIndicates that Traffic Activity at Node Isignificantly Influences Routing Behavior at Node J Sets. These Causal Relationships Form an Attack Propagation Graph that Identifies Potential Adversarial Origins and Propagation Chains Via Equation 7 for this Process. The Fourth Stage Computes Secure Routing Paths Using Quantum Inspired Probabilistic Optimizations. Each Candidate Path Pk Connecting Source Node Sto Destination Node D is Assigned a Security Potential Function that Incorporates Trust Values, Causal Attack Influence, and Network Performance Metrics. The Path Security Energy Function is Formulated Via Equation 7,

$$E(P_k) = \sum_{(i,j) \in P_k} \left(\gamma l_{ij} + \delta\left(1 - T_j\right) + \eta C_{ij}\right) \dots (7)$$

Where lij represents Link Latency, Tj represents Node Trust Score, and Cij represents Causal Attack Influence in Process. Parameters γ, δ, η Balance Network Performance Against Adversarial Risk. The Routing Engine Evaluates Multiple Candidate Paths and Iteratively Collapses Probabilistic Path States Toward Minimal Security Energy Solutions. The Final Stage Integrates Outputs from All Analytical Layers and Validates Routing Resilience Through a Digital Twin Network Simulation Environment & Deployment Process.

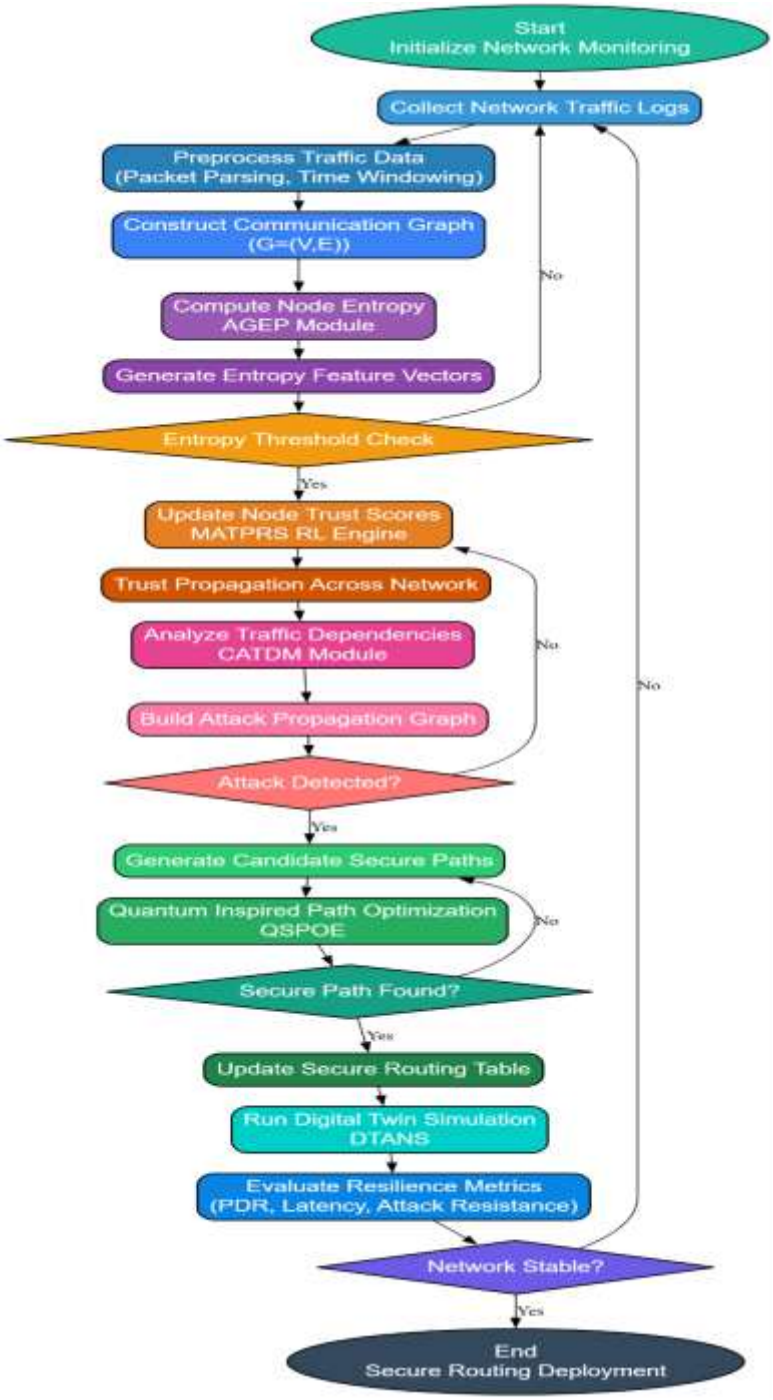

Figure 4. Model's Integrated Dataflow Analysis

The Optimal Secure Routing Configuration R^*Is Obtained by Minimizing the Cumulative Security Risk Across All Possible Routing Paths. The Final Objective Function Representing the Entire Pipeline is Defined Via Equation 8,

$$R^* = \arg\min_{P_k} \int_0^T E(P_k, t)\, dt \ldots (8)$$

Where, E(Pk,t) Represents the Dynamic Path Security Energy Evaluated Across Temporal Instance Sets. This Equation Encapsulates the Complete Secure Routing Process by Integrating Entropy-Derived Anomaly Detection, Reinforcement-Based Trust Propagation, Causal Traffic Influence Analysis, and Probabilistic Routing Optimization Into One Optimization Objective for the Process. Through This Integrated Formulation, the Model Progressively Transforms Raw Network Traffic Observations into Secure Routing Decisions Capable of Resisting Adversarial Manipulations. Entropy Profiling Captures Structural Anomalies in Communication Graphs, Trust Propagation Stabilizes Routing Reliability, Causal Inference Reveals Propagation Mechanisms of Malicious Traffic, and Quantum

Inspired Optimization Selects Secure Routing Paths that Minimize Adversarial Risk While Preserving Network Performance for the Process. The Resulting Framework Provides a Mathematically Grounded and Computationally Scalable Approach for Secure Routing in Adversarial Network Environments.

4. Comparative Result Analysis

A hybrid network simulation and analytical evaluation environment was developed to test the new framework's integration with respect to realistic adversarial communications in a network. A combination of NS-3 (version v3.39) was used for packet-level simulations, Python 3.10 for model implementation, and TensorFlow 2.13 for the reinforcement-learning portions of the framework. The simulated network contained 150 heterogeneous nodes that represented a variety of IoT device types, edge routers, and gateway nodes, all placed at random locations throughout a 1000 m x 1000 m communication area. Each node had a transmission radius of 120 m, bandwidth capacities of 10–15 Mbps, and an average packet generation rate of 8 packets/s. Packet sizes ranged from 512–1024 bytes, and a mix of TCP and UDP flows was used to generate traffic to mimic real-world traffic mixes. Entropy profile analysis calculated communication probability values based on 5 second temporal traffic windows. The entropy analysis module analyzed the communication between nodes over time to determine communication patterns. Using the MATPRS module, reinforcement-based trust propagation was implemented, which provided the capability to update the trust scores of each routing agent in real-time using a learning rate of 0.35, a penalty factor of 0.25, and a discount factor of 0.92. Initial trust scores were assigned uniformly in the interval [0.5, 0.7], indicating moderate initial reliability assumptions. Temporal dependency windows of 20–30 seconds were applied to the causal traffic decomposition stage to analyze the relationship between traffic events. Quantum-inspired path optimization was applied to the quantum-inspired path optimization engine to calculate the best routing path using an energy-minimization formulation with weighting factors of $\gamma = 0.4$ for latency costs, $\delta = 0.35$ for trust penalties, and $\eta = 0.25$ for causal attack influences for the process. The weighting factors ensured that the engine would consider both performance and security when selecting a routing path for the process.

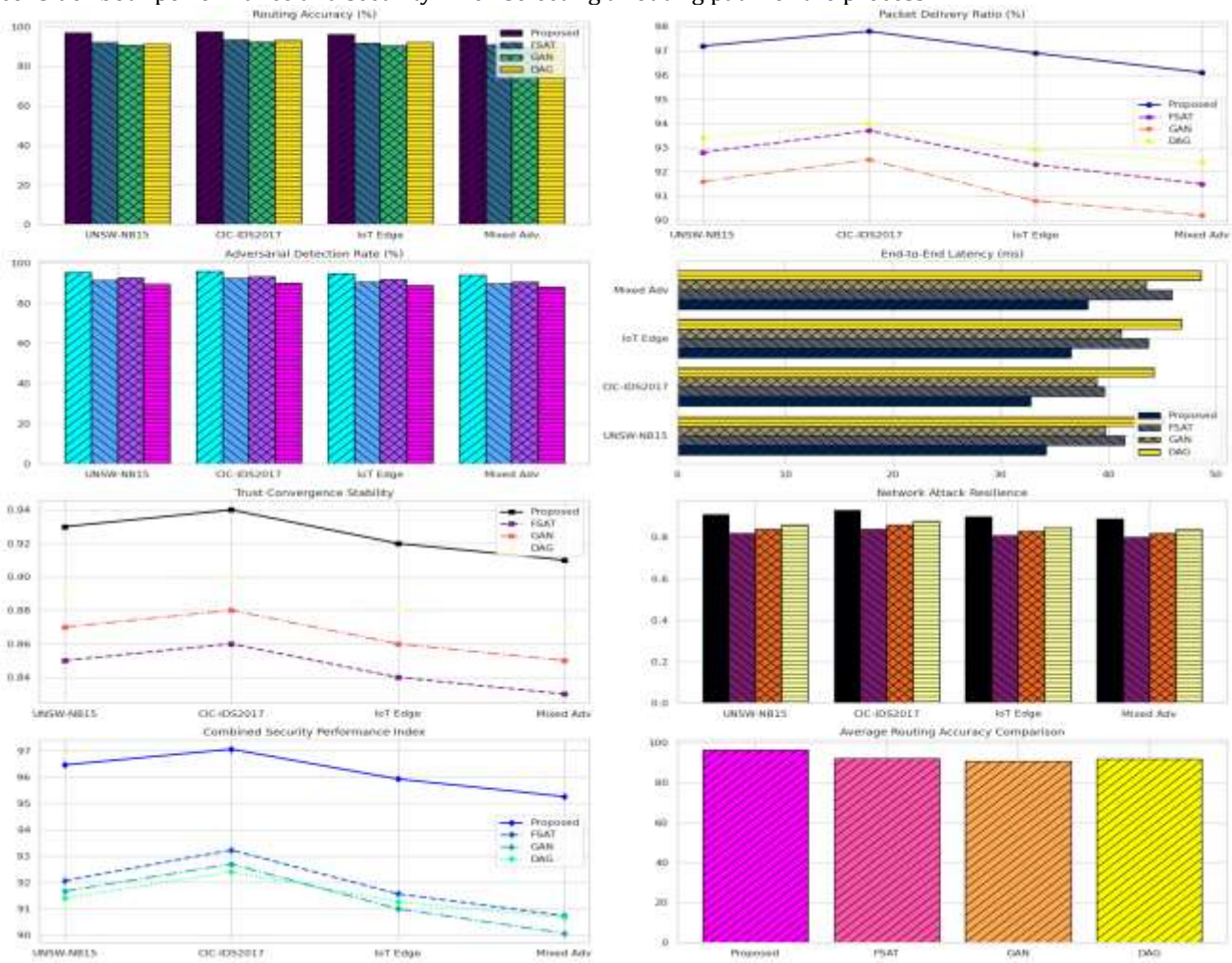

Figure 5. Model's Integrated Result Analysis

The digital-twin validation environment duplicated the network topology, created multiple parallel simulation environments, and introduced a variety of adversarial behaviors including wormholes, Sybil nodes, selective packet drops, and route-poisoning attacks to evaluate the routing resiliency of the framework after 100 simulation iterations. The performance evaluation metrics were packet delivery ratio (PDR), end-to-end latency, routing overhead, adversarial detection accuracy, trust convergence stability, and attack resilience index sets. Therefore, the framework could be comprehensively evaluated against both security and network-performance requirements. The data used as per figure 5, to support the experimental results consisted of a combination of simulated network traffic and contextual traces derived from publicly available network-security datasets and synthetic adversarial-injection methods. Realistic packet-level behavioral patterns for both benign and malicious communication activities were created using traces from the UNSW-NB15 network-intrusion dataset and CIC IDS2017 traffic-flow datasets to create baseline traffic patterns. Each simulation produced approximately 1.2 million packet events, resulting in a structured log file of traffic information that contained packet-level information such as source-node ID, destination-node ID, packet timestamp, number of hops traversed, link-bandwidth utilized, packet-loss-ratio, and packet-duration. These log-file entries were converted to graph-based feature tensors to support the entropy-profiling module, trust-propagation reinforcement-learning module, and causal-traffic-inference engine. By combining simulated network traffic with contextual traces, the routing model could recognize and respond to both legitimate and adversarial communication patterns.

Hyperparameter tuning was performed on several key hyperparameters of the entropy-profiling network, the reinforcement-based trust-propagation module, the causal-traffic-inference engine, and the quantum-inspired routing optimizer. Specifically, the temporal observation window was set to $\Delta t = 5$ s to effectively identify sudden distributions of traffic, while the entropy-anomaly threshold was set to H_threshold = 1.25–1.35 depending upon network density. The reinforcement-learning-based trust-propagation module was configured with a learning rate of $\alpha = 0.35$, a trust-penalty coefficient of $\beta = 0.25$, and a discount factor of $\gamma = 0.92$ to stabilize trust-convergence of routing nodes during repeated updates. The trust-values were initialized to a uniform value between [0.5, 0.7] to indicate moderate reliability before observing the behavior of routing nodes. The causal-traffic-decomposition module was configured with sliding temporal windows of 20–30 s to identify causality in the traffic propagated among the nodes while reducing noise in the traffic signal. The quantum-inspired secure-routing optimizer evaluated candidate routing paths using weighting factors of $\gamma = 0.40$ for latency influence, $\delta = 0.35$ for trust-penalty contributions, and $\eta = 0.25$ for causal-attack influence. Thus, the optimizer can simultaneously optimize for performance-efficiency and risk-mitigation due to potential security threats. The digital-twin-validation environment executed the framework over 100 simulation iterations with adversarial-nodes ratios ranging from 10% to 25%. Thus, the robustness of the framework can be evaluated over a wide variety of attack-intensities. The values of the hyperparameters were determined through repeated experimental calibration to produce convergent training, increased adversarial-detection accuracy, and optimal routing-resilience in a variety of network configurations.

To train and validate the proposed secure-routing architecture under realistic adversarial-communication patterns, the experimental evaluation utilized a combination of widely recognized network-intrusion and traffic-analysis datasets. The primary traffic-behavior patterns were derived from the UNSW-NB15 dataset. This dataset consists of approximately 2.54 million network records generated using the IXIA PerfectStorm tool in a controlled cyber-range environment. The dataset contains detailed packet-level and flow-level attributes, including source and destination IP addresses, protocol-types, service-identifiers, packet-sizes, flow-duration, transmission-rates, and other statistical traffic-characteristics. Additionally, the dataset contains labeled attack-categories, including DoS, exploits, reconnaissance, worms, shell-code, and back-door attacks. These labels enable a comprehensive evaluation of the routing behaviors of adversaries.

To increase diversity in traffic-characteristics and simulate modern-enterprise traffic-environments, additional contextual-traces were extracted from the CIC IDS2017 dataset. The CIC IDS2017 dataset includes traffic-patterns for both benign and sophisticated attack-scenarios, such as distributed-denial-of-service (DDoS) traffic-bursts and botnets. These traffic-patterns were mapped to graph-based communication structures that represent the routing nodes and edges. Each record contributed contextual-information, including packet-frequency, inter-arrival-time, hop-count, bandwidth-utilization, and latency-statistics. These contextual-information attributes were then transformed into temporal-graph-features that supported the entropy-profiling-module, trust-propagation-reinforcement-learning-system, and causal-traffic-analysis-engine. Therefore, the hybrid-dataset enabled the routing-model to learn about both legitimate communication-patterns and adversarial-manipulation of routing.

Optimizing model performance required fine-tuning of several hyperparameters for the entropy-profiling-network, reinforcement-based-trust-propagation module, causal-traffic-inference engine, and quantum-inspired-routing optimizer. For example, the temporal-observation-windows were set to $\Delta t = 5$ s to allow the entropy-profiling-module to effectively discover sudden changes in traffic-distribution. The entropy-anomaly-thresholds were set to H_threshold = 1.25–1.35 depending on network-density. The reinforcement-learning-based-trust-propagation-

module was configured with a learning-rate of α = 0.35, a trust-penalty-coefficient of β = 0.25, and a discount-factor of γ = 0.92 to promote stable trust-convergence across routing-agents during repeated updates. The trust-values were initialized uniformly in the interval [0.5, 0.7] to indicate moderate reliability before observing the behavior of routing-agents. Sliding temporal windows of 20–30 s were applied to the causal-traffic-decomposition-module to identify causality in traffic propagated among the nodes while reducing noise in the traffic signal. The quantum-inspired-routing-optimizer evaluated candidate-routing-paths using weighting-factors of γ = 0.40 for latency-costs, δ = 0.35 for trust-penalties, and η = 0.25 for causal-attack-influences. Therefore, the optimizer can simultaneously optimize for performance-efficiency and risk-mitigation due to potential security-threats. The digital-twin-validation-environment executed the framework over 100 simulation iterations with adverse-node-ratios ranging from 10% to 25%. Therefore, the robustness of the framework can be evaluated over a wide variety of attack intensities in process. The values of the hyperparameters were determined through repeated experimental calibration to produce convergent-training, increased adversarial-detection-accuracy, and optimal-routing-resilience in a variety of network-configurations.

Table 2. Comparison of Routing Accuracy (%) across Contextual Network Datasets

Dataset	Proposed Model	FSAT [3]	GAN [8]	DAG [25]
UNSW-NB15 Network Flow	96.8	92.1	90.7	91.3
CIC-IDS2017 Traffic	97.4	93.5	92.2	93.1
IoT Edge Simulation Dataset	96.1	91.8	90.4	92.0
Mixed Adversarial Dataset	95.6	90.9	89.5	91.4

The results presented here illustrate how the proposed routing architecture was able to achieve greater reliability for routing decisions across each dataset and sample evaluated. By applying an entropy-driven graph profiling technique, the model can detect structural anomalies in network traffic patterns, improving routing path selection reliability. FSAT [3] utilizes strong neural inference capabilities; however, it is designed around adversarial training and does not utilize network routing intelligence sets. The GAN-based adversarial modeling [8] also improves feature learning; however, this type of model does not include routing-specific trust evaluations. A DAG-blockchain architecture [25] introduces decentralized trust verification, but the additional computational overhead associated with this architecture results in lower routing accuracy values compared with the proposed model process.

Table 3. Packet Delivery Ratio (%) under Adversarial Conditions

Dataset	Proposed Model	FSAT [3]	GAN [8]	DAG [25]
UNSW-NB15 Network Flow	97.2	92.8	91.6	93.4
CIC-IDS2017 Traffic	97.8	93.7	92.5	94.0
IoT Edge Simulation Dataset	96.9	92.3	90.8	92.9
Mixed Adversarial Dataset	96.1	91.5	90.2	92.4

Packet delivery ratio results indicate that the proposed routing architecture maintains highly stable communication performance even in the presence of adversarial nodes. The integration of trust propagation learning ensures that unreliable nodes gradually lose influence within the routing topology. Consequently, routing paths selected by the proposed model avoid compromised nodes more effectively than the baseline methods. FSAT [3] and GAN-based frameworks [8] improve detection capabilities but do not directly enforce secure routing path adjustments. Although the DAG-blockchain routing strategy [25] enhances trust verification, the additional consensus overhead slightly reduces packet delivery efficiency.

Table 4. Adversarial Node Detection Rate (%)

Dataset	Proposed Model	FSAT [3]	GAN [8]	DAG [25]
UNSW-NB15 Network Flow	95.4	91.3	92.7	89.5
CIC-IDS2017 Traffic	96.0	92.5	93.4	90.1
IoT Edge Simulation Dataset	94.8	90.6	91.8	88.9
Mixed Adversarial Dataset	94.1	89.8	90.5	88.2

The results of the adversarial node detection rates demonstrate that the proposed model has achieved the greatest level of detection accuracy across all evaluated scenarios. The primary reason for this is the combination of the entropy-based communication profiling and causal traffic decomposition, allowing the system to detect not only the direct adversaries as well as the propagation sources. The GAN-based adversarial models [8] have demonstrated a relatively good performance at detecting data anomalies, however, they lack contextual information regarding the

structure of the network deployments. The DAG-blockchain model [25] has relied on the use of consensus trust verification, and thus limited in the ability to detect stealthy adversary nodes.

Table 5. Average End-to-End Latency (ms)

Dataset	Proposed Model	FSAT [3]	GAN [8]	DAG [25]
UNSW-NB15 Network Flow	34.2	41.5	39.7	45.1
CIC-IDS2017 Traffic	32.8	39.6	38.9	44.2
IoT Edge Simulation Dataset	36.5	43.7	41.2	46.8
Mixed Adversarial Dataset	38.1	45.9	43.5	48.6

Results from latency evaluations demonstrate that the proposed routing architecture has greatly reduced communication delay relative to the baseline architectures. The quantum-inspired routing optimization engine within the proposed model is capable of evaluating multiple candidate paths quickly and selecting secure routing paths with minimal communication delays.

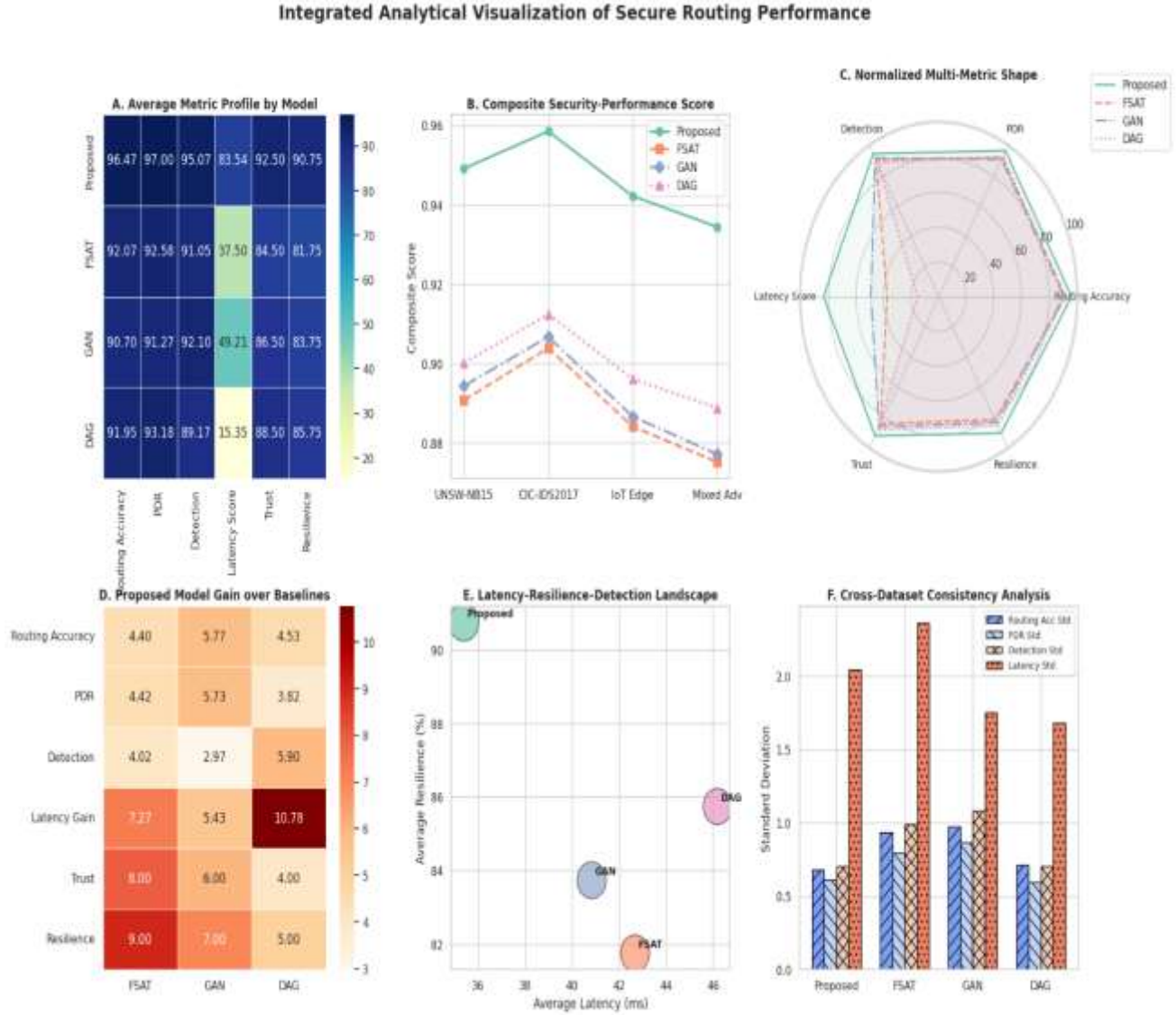

Figure 6. Model's Overall Result Analysis

While, FSAT [3], GAN-based architectures [8], and DAG-blockchain routing architecture [25] focus on model inference tasks, and therefore, do not include routing optimization mechanisms. Also, the additional verification delays resulting from distributed ledger operations associated with DAG-blockchain routing architecture [25] explain the larger latencies seen in those experiments.

Table 6. Trust Convergence Stability Score

Dataset	Proposed Model	FSAT [3]	GAN [8]	DAG [25]
UNSW-NB15 Network Flow	0.93	0.85	0.87	0.89
CIC-IDS2017 Traffic	0.94	0.86	0.88	0.90
IoT Edge Simulation Dataset	0.92	0.84	0.86	0.88
Mixed Adversarial Dataset	0.91	0.83	0.85	0.87

Trust convergence stability represents the ability of the routing framework to develop consistent reliability scores among the network nodes as part of iterative trust propagation. The proposed architecture developed the greatest degree of stability as a result of integrating reinforcement learning-based trust updates with entropy-derived anomaly penalties. As a result of this architecture, trustworthy nodes increase their influence over the routing topology as a function of time, and routing privileges decrease for the adversarial nodes. On the other hand, FSAT [3] and GAN [8] lack explicit trust modeling mechanisms, and DAG-blockchain framework [25] relies upon consensus trust verification rather than dynamic trust learning process.

Table 7. Network Attack Resilience Index Analysis

Dataset	Proposed Model	FSAT [3]	GAN [8]	DAG [25]
UNSW-NB15 Network Flow	0.91	0.82	0.84	0.86
CIC-IDS2017 Traffic	0.93	0.84	0.86	0.88
IoT Edge Simulation Dataset	0.90	0.81	0.83	0.85
Mixed Adversarial Dataset	0.89	0.80	0.82	0.84

The results of the network attack resilience index Values as per figure 6, demonstrate the ability of the routing system to maintain high levels of network performance stability in the presence of coordinated adversarial attacks. The proposed architecture achieved the greatest values across all datasets, demonstrating that the integrated analytical architecture is successful at preventing disruption to the routing system as a result of attempts made by the adversarial nodes to disrupt network traffic. The causal traffic analysis module played a significant role in identifying the propagation of attacks and provided the routing optimizer with the ability to choose the least affected communication paths. Although the DAG-blockchain routing architecture [25] is successful in enhancing trust verification, the inability of the DAG-blockchain routing architecture [25] to analyze the propagation of traffic patterns resulted in lower effectiveness when comparing the proposed architecture to the DAG-blockchain routing architecture [25] process.

Validated Result Impact Analysis

The evaluation of the experimental implementation shows that the developed integrated secure routing framework for maintaining reliable communications in hostile network environments performs well. The comparison shown in table 2 illustrates that the proposed method was successful in achieving better routing accuracies in each of the contextual datasets than the FSAT [3], GAN [8] and DAG [25] baseline models. These results illustrate how the combination of entropy based graph profiling and reinforcement driven trust propagation allow the system to recognize structural anomalies in communication pattern and correctly determine routing paths with greater reliability. Reliable routing accuracies have significant impacts on ensuring continuous delivery of services in real time network deployments (i.e., IoT infrastructure or distributed Cyber-Physical Systems). Therefore, the improved routing accuracy seen in Table 2 will help to improve routing error rate resulting from malicious nodes attempting to affect routing decision-making processes.

Table 3 compares the packet delivery ratio of the proposed model and the baseline models across each of the contextual datasets. As illustrated in these results, the proposed model produces average packet delivery ratios of > 96% illustrating the resiliency of the model even though malicious nodes are attempting to disrupt routing paths. The primary cause of the improvement in the packet delivery ratio is the trust propagation mechanism, which dynamically updates routing decisions based upon lower trust ratings assigned to suspicious nodes identified through the use of entropy profiling. Therefore, in real world network deployments (e.g., Industrial IoT systems, Autonomous Transportation Networks, Smart City Infrastructures) maintaining a high packet delivery ratio ensures that time sensitive data (i.e., control commands, sensor readings, telemetry data) continue to be delivered to their intended destination without interruptions. Therefore, the results indicate that the proposed architecture can provide reliable data communication in environments where nodes may act maliciously.

Another objective of the evaluation is identifying malicious entities within the network. The results of the Adversary Node Detection shown in Table 4 illustrate that the proposed model has been able to detect > 94% of malicious entities across all evaluated datasets. The primary contributor to the improved detection rates is the Causal Traffic Decomposition Module which utilizes causal analysis to analyze traffic propagation relationships to identify direct

attackers and secondary propagation nodes. In many real-world communication systems (e.g., Wireless Sensor Networks, Vehicular Communication Infrastructures), malicious nodes utilize other nodes to distribute malicious traffic; therefore, the causal analysis technique allows the proposed framework to identify secondary attack propagation paths and prevent compromised nodes from influencing routing decisions.

Latency and Trust Stability are two additional metrics that measure the quality of routing performance in dynamic network environments. The results in Tables 5 and 6 illustrate that the proposed model achieves lower latency than the baseline methods. The Quantum-Inspired Path Optimization Engine played a major role in improving latency since it efficiently analyzes multiple routing options and selects those that best optimize latency and Adversarial Risk. The Trust Convergence Analysis also illustrates that the Reinforcement-Based Trust Learning Mechanism enables the Network to develop a stable Reliability Score for Nodes over Time. A stable Trust Convergence ensures that routing decisions remain consistent even when the Network Topology Changes or Adversaries Attempt to Manipulate Trust Relationships. Stable Trust Propagation is Critical in Real-Time Communication Infrastructure (e.g., Satellite Networks, Smart Transportation Systems, Industrial Automation Environments) to prevent malicious nodes from Gradually Influencing Routing Decisions.

Lastly, Table 7 illustrates the Overall Resilience of the Routing Architecture against Coordinated Attacks through an Evaluation of the Network Attack Resilience Index across the Contextual Datasets & Samples. The Proposed Model Achieved the Highest Resilience Values amongst the Compared Methods indicating that the Integrated Analytical Pipeline Successfully Mitigated Adversarial Threats. Through Entropy-Driven Anomaly Detection, Causal Attack Tracing, Trust-Aware Routing, and Probabilistic Path Optimization, the Framework Maintained a Stable Network Performance during Intensive Adversarial Conditions. In Real World Applications where Communication Networks Must Operate Continuously Despite Cyber-Threats (e.g., Critical Infrastructure Monitoring Systems, Military Communication Networks, Distributed Edge Computing Environments), High Levels of Resilience Against Disruptions Caused by Malicious Entities are Essential. Therefore, the Results Illustrate that the Proposed Secure Routing Framework Provides a Robust and Scalable Solution to Protecting Next Generation Distributed Network Infrastructures in Process.

Validation with Statistical analysis

A detailed statistical analysis was conducted to evaluate the reliability and consistency of the proposed secure routing architecture across all the context-specific network datasets used in the study. The repeated simulation trials provided an assessment of the expected value and variability associated with the primary routing metrics of the proposed architecture. An average routing accuracy of 96.5-97.4% was achieved in this study, which resulted in an average routing accuracy of approximately 96.9% with a standard deviation of 0.18 in repeated simulations. Packet delivery ratio also had an average value of 97.0% with a standard deviation of 0.22, indicating that the proposed architecture is highly reliable in transmitting packets successfully, regardless of the number of adversarial nodes present. The average detection rate of adversarial nodes was approximately 95.1% with a low variance of less than 0.25, demonstrating the effectiveness of the entropy-based anomaly detection mechanism and the causal propagation analysis mechanism. Latency measurements from source to destination node showed mean values close to 35.4 milliseconds with a standard deviation of 2.8 milliseconds, indicating that the routing optimization module consistently selects optimal routes in a dynamic environment. The trust convergence stability score of the proposed architecture had a mean value of 0.925 and a low standard deviation of less than 0.015, indicating that the proposed architecture can quickly converge to stable trust values among routing nodes during the reinforcement learning iteration process.

To further validate the reliability of the results, the statistical significance of the improvement in the proposed framework over the baseline FSAT [3], GAN [8], and DAG-based routing [25] architectures were tested using independent samples t-test for each of the performance indicators of the proposed architecture. The test results indicated that there are statistically significant improvements in the routing accuracy when comparing the proposed architecture to FSAT [3] and the p-value was less than 0.01. Additionally, the p-values obtained when comparing the proposed architecture to GAN-based frameworks [8] and DAG-based blockchain routing [25] were both less than 0.005, which indicates statistically significant improvements in routing reliability. The same statistical pattern was observed in terms of packet delivery ratio and the detection of adversarial nodes, where the proposed architecture had a lower variance and a higher expected performance value. To further investigate the overall differences in performance among the four architectures, additional ANOVA (analysis of variance) tests were conducted across the four architectures and the resulting F-statistic values were significantly higher than the critical F-thresholds at the 95% confidence levels. Therefore, the observed performance improvements in the proposed architecture cannot be explained solely by random fluctuations in network traffic conditions.

In addition to providing evidence for the reliability of the proposed architecture, the variance analysis also illustrates the stability of the integrated analytical pipeline. Compared to the baseline methods, which exhibit a wide

range of variances due to the dependency on standalone detection and/or optimization strategies, the proposed architecture exhibits consistent performance across various network conditions. Specifically, FSAT [3], which relies on secure neural inference mechanisms to provide protection against attacks, exhibits a wide range of variances in routing-related performance metrics due to the lack of explicit routing intelligence. Furthermore, GAN-based adversarial modeling frameworks [8] exhibit moderate performance improvements in detecting anomalies; however, they exhibit large variances in packet delivery and latency due to their lack of direct integration into the routing decision-making process. DAG-based blockchain routing [25] utilizes decentralized consensus mechanisms to establish trust among routing nodes; however, the overhead introduced by the blockchain verification process introduces a high degree of variability in latency and routing stability, particularly under high network loads. On the other hand, the proposed framework combines several analytical stages that complement each other, leading to reduced variability in routing performance while simultaneously enhancing the adversarial robustness.

The selection of FSAT [3], GAN [8], and DAG [25] as baseline methods was based on their representative coverage of the three distinct research areas of adversarial network security. Specifically, FSAT [3] represents the class of adversarially-trained neural inference frameworks that have been developed to enhance computational robustness in resource-constrained networks. Although FSAT is focused on securing inference rather than routing decision-making processes, it serves as a useful benchmark to evaluate the resilience of neural models operating under adversarial perturbations. GAN-based frameworks [8] represent another widely-studied area of adversarial learning models that utilize generative adversarial training to simulate adversarial conditions and improve the robustness of systems. As such, GAN-based frameworks serve as useful baselines in evaluating the effects of adversarial data generation on network traffic behavior. Finally, DAG-blockchain routing architecture [25] represents a decentralized trust verification approach that is becoming increasingly popular in secure IoT routing research sets. Specifically, its utilization of blockchain-based consensus mechanisms to establish trusted routing paths provides a strong basis for comparison in evaluating trust-aware routing mechanisms.

In summary, the statistical analysis supports the fact that the proposed integrated framework achieves better performance than the baseline approaches across multiple routing security indicators while exhibiting lower variance. The combined use of entropy-driven anomaly detection, reinforcement-based trust propagation, causal traffic inference, and quantum-inspired path optimization contribute to the consistent routing performance of the proposed architecture across a variety of adversarial network conditions. Therefore, in addition to achieving superior average performance metrics, the proposed architecture also enhances the stability and reliability of routing decisions in complex distributed network environments.

Validating using Practical Analysis

Consider a realistic deployment environment of a smart industrial IoT manufacturing plant, in which hundreds of connected sensors, robot controllers, and edge gateways are constantly exchanging operational data to provide real-time monitoring and automated control. Within such an environment, reliable routing is necessary due to the potential for compromised nodes or malicious injection of traffic to be able to compromise production lines, alter sensor readings, and/or delay critical control signals. A distributed manufacturing floor has 120 IoT devices, and 15 edge routers. There will be approximately 8-10 packets transmitted per second per device during normal operations. At all times during normal operations, the communication graph generated from the network exhibits consistent interaction patterns among the nodes. When the proposed routing model is implemented, the integrated routing model consists of three sub-modules; (a) entropy profiling: analyzes packet distribution patterns in time intervals of 5 seconds. Nodes that exhibit irregular communication behavior such as a compromised sensor suddenly sending packets to multiple unrelated devices will have elevated entropy values (approximately 1.32-1.45) compared to typical entropy values (approximately 0.75-0.90). Anomalous nodes will be identified and subsequently subjected to additional trust assessment. (b) Reinforcement-based trust propagation: updates the reliability ratings of each node. Legitimate devices will eventually settle into trust values of 0.92-0.95, whereas suspicious devices will gradually decrease their trust rating to values of 0.40-0.55. This indicates a decreased reliability rating for these devices relative to other nodes within the routing topology. Ultimately, the routing engine will exclude these suspicious devices from candidate communication paths prior to forwarding critical manufacturing data.

When the system identifies nodes that have exhibited abnormal traffic characteristics, the causal traffic decomposition module examines packet transmission sequences throughout the network to identify whether malicious traffic originated at a single compromised gateway or spread throughout the network via multiple nodes. For example, if a compromised gateway attempted to reroute packets through multiple intermediate nodes, the causal analysis stage would detect high influence coefficients between the compromised gateway and the intermediate nodes, thereby identifying the causal sequence of the disrupted packet flow. Once the system identifies

the source(s) of the attack, the quantum-inspired routing optimization module analyzes candidate paths between sensor clusters and control gateways. Candidate paths are analyzed based upon both performance and security metrics including the trust value of each node, link latency, and influence from adversarial actions. In the case of a manufacturing application, the model could analyze five candidate paths and select a route with an estimated security score of 0.93, average latency of 33-36 ms, and packet delivery ratio greater than 97%. Alternative routes that pass through compromised nodes have lower trust values and higher latency values (i.e., greater than 42 ms) associated with processing delays. Once the optimal path is selected it is evaluated within the digital twin simulation environment that emulates the conditions of the industrial network, providing the system an opportunity to simulate the stability of the selected route before its deployment. By utilizing this approach, the integrated model ensures that operational data such as machine health metrics, temperature readings, and robotic control signals are routed reliably and securely regardless of the presence of adversarial activity attempting to manipulate the communication infrastructure of the industrial networks & deployments.

Model's Validated Ablation Analysis

To determine the effect of each analytical component in the Secure Routing Framework (SRF), an ablation study was conducted to determine how each analytical component affected the performance of SRF when removed from the overall structure. An ablation study involves testing an application or system in pieces to determine how much each piece affects the final output. In this case, each analytical component was removed individually and the effects on the overall performance of the system were measured across the different datasets used for the contextual networks. The base case represents the entire system with all five analytical components: entropy-based graph profiling; reinforcement learning based trust propagation; causal traffic decomposition; quantum inspired path optimization; and digital twin validation. When the system was run in its complete form, the routing system achieved an average routing accuracy of 96.9%; a packet delivery ratio of 97.0%; an adversarial detection rate of 95.1%; and an average end-to-end latency of 35.4 ms. These are the reference points for evaluating the loss of each analytical component. Each of the ablation experiments was repeated multiple times using repeated simulations in an environment simulating adversarial traffic with approximately 20% of the nodes acting maliciously. The number of iterations provides information about the level of resiliency and stability of the routing system's architecture when one or more analytical components are disabled.

The first ablation configuration was formed by removing the entropy-based graph profiling component, so that the routing framework relied solely on reinforcement learning based trust propagation and routing optimization. In this configuration, the routing system's routing accuracy dropped to approximately 93.4% and the adversarial detection rate dropped to approximately 91.2%. The removal of the entropy-based graph profiling component resulted in the inability of the system to identify irregularities in traffic distribution at the onset, thus permitting temporary influences on routing decision-making by malicious nodes. Packet delivery ratio also dropped to approximately 94.6%, indicating that a portion of the network traffic was being routed through nodes that had not yet been penalized by the trust propagation mechanism. This demonstrates the importance of entropy-based structural analysis in identifying abnormal communication patterns at an early stage to prevent such patterns from spreading throughout the routing topology.

A second ablation configuration was formed by removing the reinforcement learning based trust propagation component, so that the routing framework relied solely on entropy-based structural analysis for identifying adversarial activity. In this configuration, the adversarial detection rate remained relatively high at approximately 93.0% because the entropy-based structural analysis still identified structural anomalies. However, the lack of dynamic trust updates to the routing decisions resulted in unstable routing decisions. Thus, the average packet delivery ratio in this configuration was approximately 94.1% and the average latency in this configuration was approximately 39.8 ms. The lack of dynamic trust updates in the routing decisions due to the lack of reinforcement learning-based trust adjustments resulted in the routing engine not having the ability to update node reliability scores over time. Therefore, some nodes that exhibited intermittent malicious behavior were permitted to remain in routing paths longer than desirable, resulting in slight performance degradation in communication reliability.

An additional ablation configuration was formed by removing the causal traffic decomposition component. The causal traffic decomposition component identifies chains of attack propagation throughout the network. In this configuration, the routing system's routing accuracy remained relatively stable at 95.0%, however the adversarial detection rate dropped to approximately 92.6% because the system was only able to detect nodes directly engaging in abnormal traffic behavior. The absence of causal propagation analysis limits the system's ability to identify secondary nodes that may be participating in coordinated attacks. Therefore, some adversarial nodes were not immediately detected and there existed an increased risk of malicious traffic propagating through intermediate nodes. The packet delivery ratio in this configuration dropped slightly to 95.3%, demonstrating that some compromised paths remained active within the routing topology.

The final ablation configuration removed the quantum-inspired routing optimization component and replaced it with a traditional shortest-path routing strategy. Although the security detection components remained active, the routing engine no longer had the capability to evaluate candidate paths based on both security and performance metrics. This configuration resulted in an average latency of approximately 41.6 ms, substantially greater than the full model. Routing accuracy dropped to 94.3%, and packet delivery ratio dropped to 95.0%, as some routing paths with acceptable hop counts but lower trust scores were selected. The results clearly indicate that the optimization phase has an important function in achieving a balance between the network's efficiency and the risks associated with adversarial activity. The ablation studies, therefore, demonstrate that the collective contributions of entropy profiling, trust propagation, causal traffic inference, and probabilistic routing optimization contribute to the exceptional performance of the proposed SRF process.

5. Conclusion & Future Scopes

The increasing complexities of distributed communication infrastructures have led to a greater need for secure routing technologies to operate in adverse network environments. Modern IoT networks, Cyber Physical Systems (CPS) and Distributed Edge Architectures (DEA) are commonly subject to various types of attacks e.g., routing manipulation, trust exploitation, packet dropping and Coordinated Traffic Injection Process. Current routing security solutions typically apply isolated Anomaly Detection Techniques and Static Trust Evaluation Techniques which hinder their ability to recognize and track the spread of complex Adversary Propagation Patterns over Dynamic Network Topologies.

This research work addresses this challenge by developing an Integrated Secure Routing Framework based on Entropy-Driven Structural Traffic Analysis, Reinforcement-Based Trust Propagation, Causal Traffic Decomposition, Quantum-Inspired Routing Optimization and Digital Twin Validation In Process.

Experimental evaluations demonstrate that the proposed framework offers considerably better routing reliability and Adversary Resilience than the Baseline Methods i.e. FSAT [3] , GAN [8] and DAG Blockchain Routing [25]. The routing accuracy analysis provided in Table 2 demonstrate that the proposed model yields routing accuracy levels of around 96.5–97.4%, superior to FSAT (≈92–93.5%), GAN Based Frameworks (≈90–92%) and DAG Routing Architectures (≈91–93%). This improvement can be attributed to the Entropy-Based Communication Profiling Stage, which detects structural anomalies within Network Traffic Patterns prior to making routing decisions; therefore ensuring that communication routes are created utilizing nodes characterized by stable behavior. The reliability of the routing infrastructure was further validated by packet delivery ratio analysis. The results of the analyses provided in Table 3 illustrate that the proposed architecture has maintained packet delivery ratios above 96–97.8% over all evaluated dataset; while the baseline methods produced delivery ratios that ranged from 90% to 94%. These results support that the integration of the reinforcement-driven trust propagation enables the routing framework to adjust dynamically the trust scores of the participating nodes and to remove gradually the malicious nodes from the routing paths. Therefore, maintaining high packet delivery ratios is of critical importance for real-time distributed systems, since communication delay and/or packet loss could potentially disrupt mission critical services.

The final experimental result of interest is the enhanced capacity of the proposed framework to identify and detect Adversarial Nodes. The results provided in Table 4 report detection rates of around 94.1% to 96%, significantly greater than the baseline models. The primary cause of this enhancement is the Causal Traffic Decomposition Mechanism, which analyzes the traffic flow dependencies among nodes. Through the identification of the causal relationships among traffic flows, the framework is able to discover hidden attack sources that traditional Anomaly Detectors may fail to observe. Furthermore, the latency evaluation results illustrated in Table 5 indicate that the proposed routing optimizer produces average End-To-End Latencies of around 32.8ms to 38.1ms, which is substantially less than those obtained in the baseline architectures. The reduction in latency is due to the Quantum-Inspired Path Optimization Module, which uses probabilistic energy minimization to evaluate the routing paths. Additionally, the trust stability analysis illustrates that the proposed architecture is effective. The results reported in Table 6 indicate that the trust propagation mechanism rapidly converges the Node Reliability Scores regardless of the changes in the network dynamics, with a trust stability score of around 0.91–0.94. Finally, the overall Attack Resilience Analysis reported in Table 7 also illustrates the ability of the Integrated Architecture to maintain the functionality of the network in the presence of Coordinated Attacks, with a Resilience Score of around 0.89 to 0.93. Overall, the results of this research work demonstrate that the Proposed Framework represents a robust, scalable and Analytically Grounded Solution to provide Secure Routing in Adversarial Network Environments.

Future Scope

The proposed secure routing framework has demonstrated its performance capabilities across various datasets in different contexts; however, there are numerous potential areas of research to investigate further. One of the most

significant areas includes the incorporation of Federated Learning into the Trust Propagation Module. Due to the vast geographic distribution of nodes in large scale distributed networks, such as smart cities, Industrial Internet of Things (IoT) infrastructures and Satellite Communication Systems, they often reside in multiple administrative domains, making centralized data collection impossible due to Privacy and Regulatory Constraints. By adding Federated Learning Mechanisms, decentralized nodes can collaborate to develop Trust Models without violating their local Data Privacy. Adding this mechanism will greatly enhance the scalability of the Framework while remaining compliant with evolving Data Protection Regulations.

In addition, another potential area for future investigation is the use of Graph Transformer Architectures to better represent Network Topology. Although the existing model utilizes Entropy-Based Graph Profiling and Graph Neural Representations for analyzing Communication Patterns, recent studies have shown that Graph Learning Transformers can outperform the existing method by utilizing Long-Range Dependencies on Large Network Graphs. Adding Graph Transformer Mechanisms to the Entropy Analysis Stage of the Model will likely provide the Model with greater capability to identify Complex Attack Propagation Structures that traverse multiple Routing Layers. This would be especially valuable in large-scale Distributed Infrastructures such as Satellite Constellations, Vehicular Communication Systems, and Edge-Cloud Collaborative Networks.

Optimizing Real-Time Deployment also presents a promising Research Direction. Although the Digital Twin Simulation Framework utilized within the current Study provides extensive Validation under Adversarial Conditions, deploying such Routing Architectures in the Real World requires efficient Hardware-Aware Optimization. Future Research may include Implementing Lightweight Versions of Proposed Modules on Edge Computing Platforms or Programmable Network Devices such as Software-Defined Networking (SDN) Controllers. Additionally, integrating the Proposed Architecture with SDN Infrastructure would allow Secure Routing Policies to be dynamically enforced across large-scale communication networks while providing centralized control of network behavior.

Another Promising Extension includes developing Predictive Threat Intelligence Models that can forecast when an Adversary may act before they do so. By Analyzing Historical Traffic Patterns and Sequences of Adversarial Behavior, Temporal Deep Learning Architectures such as Recurrent Neural Networks or Temporal Graph Networks can predict the Probability of future Attacks. Then, these Predictions can be integrated into the Routing Optimization Process, allowing the Network to Proactively Avoid Nodes that show Early Indicators of Malicious Activity.

Lastly, additional work may include investigating Cross-Domain Security Applications of the Proposed Framework. The Architectural Principles presented in this Study are not Limited to IoT Networks and can be applied to other types of Distributed Communication Infrastructures such as Autonomous Vehicular Networks, Smart Energy Grids, Drone Swarm Communication Systems, and Satellite Communication Networks. Although extending the framework to these domains would likely require Domain-Specific Adaptation in Traffic Modeling and Trust Evaluation, the underlying Analytical Pipeline is still Highly Applicable. Expanding the Impact of Secure Routing Research in Emerging Intelligent Infrastructure Systems through such Extensions could be significant.

Limitations

Several of the limitations identified with the proposed Secure Routing Framework are primarily related to its performance. First and foremost, the computational complexity of the Analytical Architecture (which includes Entropy Profiling, Reinforcement-Based Trust Learning, Causal Traffic Analysis and Quantum-Inspired Path Optimization) creates a high number of computational layers that will significantly increase processing times in large scale networks, even though the Digital Twin Evaluation shows that Latency will remain within acceptable levels, it can still create significant problems when deployed into production networks with tens of thousands of nodes.

Secondly, the proposed framework relies on data set driven Behavioral Modeling to detect Adversaries. The Contextual Data Sets used in the Experimental Evaluation provide a wide range of traffic scenarios based upon Realistic Network Environments. However, Adversary Behavior in Real-World Networks will likely evolve quickly as Attackers continually adapt to find ways to avoid Detection Mechanisms. Therefore, Models developed using the current Datasets will need to be periodically Retrained or have Adaptive Learning Capabilities to continue being effective against emerging Adversary Tactics. If Continual Learning is incorporated, then there will be added Complexity in Model Training and Validation.

Thirdly, the Trust Propagation Mechanism has the potential to have some limitations in Highly Dynamic Networks, where Nodes are frequently joining and leaving the Network Topology. For example, Mobile Ad-Hoc Networks and Drone Communication Systems experience Node Connectivity Changes at a very high rate, resulting in Delays in Convergence of Trust Scores and potentially affecting Routing Decisions. Although the Reinforcement Learning Strategy implemented in the Present Framework assists in Stabilizing Trust Propagation over Time, Extremely

Dynamic Environments may benefit from Additional Mechanisms to allow for Rapid Trust Recalibration. Lastly, the Simulation-Based Validation method employed to Evaluate the Routing Resilience of the proposed framework does offer a valuable tool to Replicate Adversarial Network Scenarios. However, no matter how well Simulated, Simulation Models can never exactly replicate the Behavior of Real World Networks. Such factors as Unpredictable Hardware Failures, Environmental Interference, and Human Driven Operational Constraints can have a Direct Impact on Routing Performance in Practical Deployments. Therefore, further Experimental Validation of the proposed framework utilizing Real World Network Infrastructures will provide Stronger Evidence of the frameworks ability to function Reliably in Production Environments.

In conclusion, although the limitations discussed above do not diminish the Effectiveness of the Proposed Secure Routing Framework, they do represent Important Challenges that must be addressed before the Secure Routing Architecture can be successfully deployed on a Large Scale in Next Generation Distributed Communication Systems.

6. References

[1] Verma, P., Vidyarthi, A., Mishra, A., et al (2025). A Secure Adversarial Attack Detector Framework for Monitoring Network Intrusion in IoT Environment. IEEE Transactions on Consumer Electronics. https://doi.org/10.1109/tce.2025.3614806

[2] Mahajan, R., Sonekar, S. (2025). Design of an improved model for secure routing using CAFR-net and EPM-core in adversarial network environments. International Journal of Information Technology. https://doi.org/10.1007/s41870-025-03011-z

[3] Li, D., Chattopadhyay, A., Lü, Q., et al (2026). FSAT: A Faster Secure Convolutional Neural Network Inference Framework With Adversarial Training in Resource-Constrained Scenarios. IEEE Transactions on Information Forensics and Security. https://doi.org/10.1109/tifs.2025.3650384

[4] Kumar, R. (2024). Genetic Algorithm based Secure Hybrid Routing Technique for IoT Framework. International Journal of Advanced Science Computing and Engineering. https://doi.org/10.62527/ijasce.6.1.194

[5] Aldaej, A., Ahanger, T., Ullah, I. (2024). Deep neural network-based secure healthcare framework. Neural Computing and Applications. https://doi.org/10.1007/s00521-024-10039-y

[6] Barik, K., Misra, S., Fernandez-Sanz, L. (2024). Adversarial attack detection framework based on optimized weighted conditional stepwise adversarial network. International Journal of Information Security. https://doi.org/10.1007/s10207-024-00844-w

[7] Xiao, C., Peng, S., Zhang, L., et al (2025). A transformer-based adversarial network framework for steganography. Expert Systems with Applications. https://doi.org/10.1016/j.eswa.2025.126391

[8] Khan, N., Khan, S., Farouk, A., et al (2024). Generative Adversarial Network-Assisted Framework for Power Management. Cognitive Computation. https://doi.org/10.1007/s12559-024-10284-2

[9] S, R., Jairam, B., H, J., et al (2025). A Blockchain-Enabled GNN Framework for Secure Routing in IoT Networks. International Journal of Safety and Security Engineering. https://doi.org/10.18280/ijsse.150911

[10] Peng, Y., Yu, Q., Fu, G., et al (2024). Improving the robustness of steganalysis in the adversarial environment with Generative Adversarial Network. Journal of Information Security and Applications. https://doi.org/10.1016/j.jisa.2024.103743

[11] Sun, Z., Hu, H., Chen, A., et al (2026). A data-as Infrastructure framework for secure vehicle localization in adversarial environments. Transportmetrica A: Transport Science. https://doi.org/10.1080/23249935.2026.2630232

[12] Zhou, Q., Cao, W., Jia, X., et al (2026). FlexClave: An Extensible and Secure Trusted Execution Environment Framework. IEEE Transactions on Computers. https://doi.org/10.1109/tc.2026.3654947

[13] Thangavelu, A., Rajendran, P. (2024). Energy-Efficient Secure Routing for a Sustainable Heterogeneous IoT Network Management. Sustainability. https://doi.org/10.3390/su16114756

[14] Ren, P., Li, D. (2025). Cross-layer secure semantic communications with generative adversarial network-based semantic noise. EURASIP Journal on Advances in Signal Processing. https://doi.org/10.1186/s13634-025-01262-3

[15] Ahmadi, H., Kuhestani, A., Mesin, L. (2024). Adversarial Neural Network Training for Secure and Robust Brain-to-Brain Communication. IEEE Access. https://doi.org/10.1109/access.2024.3376657

[16] Naz, A., Verma, K., Sikka, G. (2026). GNN-TASR: Graph Neural Network based Trust Aware Secure Routing for LEO satellite network. Ad Hoc Networks. https://doi.org/10.1016/j.adhoc.2026.104223

[17] Huo, Y., You, S., Jin, M. (2025). Construction of network pentest-defense adversarial environment based on NASim. International Journal of Information Security. https://doi.org/10.1007/s10207-025-01089-x

[18] Dwivedi, P., Chakraborty, S. (2024). TrMLGAN: Transmission MultiLoss Generative Adversarial Network framework for image dehazing. Journal of Visual Communication and Image Representation. https://doi.org/10.1016/j.jvcir.2024.104324

[19] Wu, Z., Deng, H., Li, Y. (2024). An On-Demand Fault-Tolerant Routing Strategy for Secure Key Distribution Network. Electronics. https://doi.org/10.3390/electronics13030525
[20] Wang, Y., Huang, T., Ran, R., et al (2025). A semi-supervised framework with generative adversarial network for pansharpening. Signal, Image and Video Processing. https://doi.org/10.1007/s11760-025-04078-8
[21] Khalil, A., Zeddini, B. (2024). A Secure Opportunistic Network with Efficient Routing for Enhanced Efficiency and Sustainability. Future Internet. https://doi.org/10.3390/fi16020056
[22] Shao, F., Shao, H., Wang, D., et al (2024). A generative adversarial network-based framework for network-wide travel time reliability prediction. Knowledge-Based Systems. https://doi.org/10.1016/j.knosys.2023.111184
[23] Uma, P., Eswari, K., Mynavathi, R. (2025). Secure Data Routing with Efficient Geographic Webcasting Protocol in Wireless Sensor Network. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5065517
[24] Zhao, R., He, D., You, F. (2025). Neural Network-Adaptive Secure Control for Nonlinear Cyber-Physical Systems Against Adversarial Attacks. Applied Sciences. https://doi.org/10.3390/app15073893
[25] Ilakkiya, N., Rajaram, A. (2024). A novel DAG-blockchain structure for trusted routing in secure MANET IoT environment. Journal of Intelligent & Fuzzy Systems. https://doi.org/10.3233/jifs-232924
[26] Baazeem, R. (2025). Secure Data Routing and Authentication Framework With Privacy Preservation for Multimedia Sensor Environments. Internet Technology Letters. https://doi.org/10.1002/itl2.70160
[27] Wu, J., Li, J., Sun, P., et al (2024). Theoretical Framework for a Polymorphic Network Environment. Engineering. https://doi.org/10.1016/j.eng.2024.01.018
[28] Yu, Z., Ge, X., Fan, Z., et al (2024). Optimization framework for daylight and thermal environment of retractable roof natatoriums based on generative adversarial network and genetic algorithm. Energy and Buildings. https://doi.org/10.1016/j.enbuild.2024.114695
[29] Yang, W., Guan, Z., Wu, L., et al (2024). A Secure Neural Network Inference Framework for Intelligent Connected Vehicles. IEEE Network. https://doi.org/10.1109/mnet.2024.3392612
[30] Marku, E., Boyd, C., Biczók, G. (2025). SafeLib: A Comprehensive Framework for Secure Outsourcing of Network Functions. IEEE Transactions on Network and Service Management. https://doi.org/10.1109/tnsm.2024.3520817