International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/25 Volume 12, Issue 3, May – June (2025)

RESEARCH ARTICLE

Design of an Improved Model for Secure and Efficient Wireless Routing Using HFAH-RSA-HE and MAPS-AOMDV Process

Minal Ghute
Department of Electronics, Yeshwantrao Chavan College of Engineering, Nagpur, India.
✉ mrsminalghute@gmail.com

Yogesh Suryawanshi
Department of Electronics, Yeshwantrao Chavan College of Engineering, Nagpur, India.
yogesh_surya8@rediffmail.com

Received: 24 March 2025 / Revised: 24 May 2025 / Accepted: 04 June 2025 / Published: 30 June 2025

Abstract – To handle drawbacks of existing models, the proposed Hierarchical Federated Adaptive Secure Routing for Wireless Networks integrates encryption and intelligent routing. The security component HFAH-RSA-HE introduces a hierarchical federated homomorphic RSA scheme where the encryption depth can adapt to the energy level of the nodes-high-energy nodes use full homomorphic encryption while low-energy nodes can use various partial ones-thus, cutting encryption latency and energy burden by 40%. Routing is performed under Multi-Agent Predictive Swarm-AOMDV MAPS-AOMDV search to optimize AOMDV, whereas the swarm intelligence and reinforcement learning provide the ability to predict link failures in real-time and congestion-aware multipath selection. With this, packet delivery ratio is improved by 10% with a 40% reduction on delay, and 40% improvement on network lifetime. HFA-SRWN has thus gained energy-aware security and adaptive routing, which makes it a candidate for IoT, MANETs, and UAV networks.

Index Terms – Secure Routing, Homomorphic Encryption, Multi-Agent Reinforcement Learning, AOMDV, Energy Efficiency, Process.

1. INTRODUCTION

Wireless communication systems in environments characterized by dynamics and limited resource constraints such as MANETs, IoT, and UAV networks suffer unique bottlenecks in energy efficiency, security, and reliability. Within such networks [1, 2, 3], the optimization of routing protocols vis-a-vis their encryption mechanisms is paramount if the system is to remain efficient, protecting the sensitive data therein from would-be security threats. The conventional routing protocols are poor in gradient performance tradeoffs between least energy consumption and maximum end-to-end security. Such failure leads to high packet loss, delays in transmissions, and unauthorized data reach. The intrinsic trade-off between the security of encryptions and cost in computation is a big challenge in wireless communications. Classical types of encryption schemes under rigorous postulations are extremely computationally expensive and can therefore place an overwhelming burden on resource depleted equipment. These schemes also often create a bottleneck in performance in terms of deteriorating network latency and throughput. And to solve these issues [4, 5, 6], it is also very important to have intelligent routing protocols that would address predicting link failures and optimizing multi-path routing, so as to reduce delays and packet losses. However, many of the existing solutions do not predict and manage congestion and the reliability of links in real time, leading to poor routing choices and increased loss of packets. To address these challenges, the proposed work introduces a new framework integrating Hierarchical Federated Adaptive Homomorphic RSA Encryption (HFAH-RSA-HE) for secure data transmission with multi-agent predictive swarm-based AOMDV (MAPS-AOMDV) routing mechanisms. Such integration allows the system to dynamically adjust its depth of encryption according to nodes' energy availability for maximal energy efficiency while not compromising considerably on security. Elevating the adaptive and congestion-aware capability of MAPS-AOMDV meanwhile ensures that routing decisions set the stage for reduced delays, improved packet delivery ratio, and extended network lifetime sets.

Wireless communication technologies will have emerged as a cornerstone in modern computing, with a kind of infrastructure that includes the Internet of Things (IoT), Mobile Ad hoc Networks (MANETs), and Unmanned Aerial Vehicle (UAV) systems into the process. These systems have limited energy resources, wide-open transmissions, and always-dynamic topologies, thus making them vulnerable in process. The primary public concern in such cases is to

RESEARCH ARTICLE

provide the sensitive data protection and to ensure that the effective routing to adapt to the changes in the network conditions would be done for the process. Traditional cryptographic techniques, although quite secure, are computationally intensive in process. On the contrary, almost all routing protocols fail to anticipate situations of data congestion and link instability sets. To mitigate these dual challenges, the present study blends multipath routing sets with homomorphic encryption while assisted by reinforcement learning process. This research advances a federated model with balance in the energy perspective, capturing simultaneously the cryptographic intensity and routing behavior depending on the real-time changes in security levels-comforting with performance efficiency in different wireless environments.

1.1. Problem Statement

In today's scenario, routing efficiency and data security contradict each other in most cases in wireless networks, particularly for those highly dynamic and energy-constrained conditions such as IoT networks and MANETs. Full-blown cryptographic protocols introduce considerable latency to any computation, while simple routing schemes usually do not adjust to real-time remapping due to link failure and congestions. Centralized models are really not appropriate because of the decentralized nature of these networks. This study concerned the design of a lightweight, adaptable, and decentralized routing protocol that could simultaneously offer a proper trade-off between security and performance using federated homomorphic encryption and predictive multipath routing.

1.2. Motivation and Contribution

The motivation for this work arises from the highly critical need for secure, efficient, and resilient communication in wireless networks, especially when the nodes are resource-constrained or limited in energy capability. Conventional paradigms for secure wireless communication often could not balance the trade-off between security, energy efficiency, and routing performance. The use of homomorphic encryption would be secure but adds a lot of computational overhead, rendering it too computationally intensive to be feasible in a resource-constrained environment without major modifications. Also, routing protocols such as AOMDV do not provide for any forward-looking adjustments to take place on link failures in real time, rendering them incapable of quickly responding to link failures and perhaps degrading performance. All these said issues underscore the imperative for inventive solutions that tackle security and routing efficiency in an integrated manner in the ongoing process. We have contributed principally to the formation of the HFA-SRWN model, which mixes HFAH-RSA-HE and MAPS-AOMDV, applying these features to solve the problems already faced by existing solutions. First, the HFAH-RSA-HE model optimizes homomorphic encryption through a hierarchical architecture capable of adapting its encryption depth to the node capabilities, drastically reducing unnecessary computational complexity. Thus, energy-rich nodes use full-homomorphic encryption for maximum security, whereas battery-constrained nodes employ partially homomorphic encryption to balance security with energy cost. This way adaptive encryption minimizes energy wastage and yet preserves the integrity of the data samples.

Second, the MAPS-AOMDV routing model integrates multi-agent reinforcement learning and swarm intelligence for tracking link failure predictions and dynamically optimizing routing decisions. By predicting link failure dynamically and optimizing routing decisions, it allows the network to adjust its routing paths proactively to maintain low end-to-end delay, increase packet delivery ratio, and prolong network lifetime. The model reinforces low-congestion stable paths using a pheromone-based approach and reroutes traffic dynamically before boundary failures occur, helping minimize packet loss and maximizing throughput. This is a very major advancement in the field: presenting a comprehensive solution to the problems of secure and efficient routing in wireless networks. Below are some points that can reinforce HFA-SRWN as an exemplary touchstone-model of the future wireless communication protocols especially with massive applications in IoT, MANET, and UAV sets.

The rest of the paper is organized as follows. Section 2 presents a comprehensive review of related work, discussing existing methodologies and their limitations. Section 3 provides a detailed description of the proposed model, including its architecture, key components, and the underlying algorithms employed. Section 4 outlines results and discussions to assess the model's performance. Finally, Section 5 concludes the paper and suggests potential directions for future research.

2. RELATED WORK

Significant advancements have been made over the years with the evolution of the secure and efficient routing in wireless networks, with much recent research focusing on optimizing security with energy efficiency in adaptive routing mechanisms. With the increasing trend in the emergence of IoT, MANET, and UAV networks, there is dire need for robust security frameworks and intelligent routing mechanisms. This review, based on recent research papers, gives an extensive elaboration on recent methodologies tackling key challenges presented in wireless communications, mainly encryption overheads, multipath selection, and attack resilience. The considered papers span the last couple of years, offering an insightful chronological progression over the techniques in the domain. Early contributions by Fei et al. [1] presented an energy-efficient QoS secure routing algorithm that provides a clear path for

RESEARCH ARTICLE

incorporating energy-awareness into security mechanisms. Murthy et al. [2] further enhanced this work by putting in a hybrid moth flame-shark smell optimization algorithm for improving wireless security especially for IoT networks. Sharma et al. [3] and Kumar and Sharma [4] on trust-based routing and sustainable network security accentuated the necessity of multi-level trust mechanisms against routing attacks. This has made way to Godi et al. [5] who issued an optimization-based cluster head selection mechanism that considerably heightens energy stability in WSNs.

As security threats evolved, researchers focused on refining routing algorithms to combat attacks in MANET environments. Prasanna and Ramesh [6] explored attack prevention strategies, while Feroz Khan [7] extended this work with the Enhanced Multi-Attribute Based Trusted Attack Resistance (EMBTR) framework, specifically designed for sensor node security. Paulraj et al. [8] introduced an innovative Quantum Chimp Optimization approach, leveraging DNA sequence-based multihop routing, enhancing both security and efficiency. Addressing congestion-related security issues, Vankdothu and Hameed [9] devised a congestion-aware secure routing protocol, ensuring stable data transmission in IoT-WSN applications. A significant breakthrough came with Prabha et al. [10], who employed a dual-discriminator conditional generative adversarial network to optimize secure cluster-based routing, achieving remarkable resilience against adversarial threats. Similarly, Bai et al. [11] developed the TSRP (Trust-Based and Energy-Aware Secure Routing Protocol), demonstrating superior performance in resource-constrained environments. Bhanu and Santhosh [12] took a fuzzy logic-enhanced approach to secure multicast routing, striking a balance between security and energy preservation in WSNs. Beula and Franklin [13] further contributed with the SCMABC algorithm, enhancing secure data transmission for smart grids. In parallel, LoRaWAN-based secure routing was explored by Sharma and Daruwala [14], focusing on vehicular networks, ensuring real-time communication security.

Ananthi et al. [15] extended this by developing a trusted path selection mechanism for Internet of Medical Things (IoMT), ensuring high-security standards in critical healthcare communications. Yesodha et al. [16] introduced Elliptic Curve Encryption (ECE) in an ACO-based routing model, significantly improving cryptographic efficiency in sensor networks. Subramani and Selvi [17] merged fuzzy logic with Ant Colony Optimization (ACO), enhancing intrusion detection and adaptive routing strategies. Further expanding AI-driven secure routing, Luqman and Faridi [18] integrated Artificial Bird Optimization with Deep Learning, introducing a novel node deployment strategy for secure wireless networking. Verma and Jha [19] designed a cluster-based optimal routing framework, emphasizing security-aware energy-efficient data transmission in IoT-WSNs. Ambareesh et al. [20] adopted a coupled ensemble selection approach, leveraging type-2 fuzzy logic for robust security sets. Table 1 shows Model's Empirical Review Analysis.

Table 1 Model's Empirical Review Analysis

Reference	Method	Main Objectives	Findings	Limitations
[1]	Energy-Efficient QoS Secure Routing	Optimize security and energy efficiency in WSNs	Achieved higher throughput and energy efficiency	Scalability issues in large-scale WSNs
[2]	Hybrid Moth Flame-Shark Smell Optimization	Secure wireless communications for IoT	Improved security and reliability in IoT networks	High computational overhead
[3]	Multi-Level Trust-Based Secure Routing	Trust-based multipath routing for IoT-WSN	Enhanced attack resistance and delivery ratio	Increased routing overhead
[4]	PathGuard	Sustainable and secure routing for IoT-WSNs	Improved packet integrity with trust-based security	Requires continuous trust updates, increasing latency
[5]	Hybrid Optimization-Based Cluster Head Selection	Energy-aware and stable routing in WSNs	Reduced energy consumption and optimized multipath selection	Complexity in hybrid optimization algorithms
[6]	Attack Prevention Mechanism in MANET	Secure routing with attack mitigation	Stronger resilience to blackhole and Sybil attacks	Lacks real-time adaptation to new attack patterns

RESEARCH ARTICLE

[7]	Enhanced Multi-Attribute Trusted Attack Resistance (EMBTR)	Secure sensor node communication	Enhanced resilience against DoS and spoofing attacks	Requires higher processing power on sensor nodes
[8]	Quantum Chimp Optimization	DNA sequence-based secure routing	Achieved low latency and high data integrity	High computational cost
[9]	Congestion-Aware Secure Routing	Minimize interference and congestion in IoT-WSNs	Achieved higher transmission efficiency in congested networks	Inefficient under low-density network conditions
[10]	Dual-Discriminator GAN-Based Secure Routing	AI-driven cluster-based routing for MANETs	Improved security and adaptability	GAN training requires large datasets
[11]	Trust-Based Energy-Aware Secure Routing (TSRP)	Secure routing for resource-constrained networks	Optimized security-energy trade-off	Performance degrades with high node mobility
[12]	Fuzzy Enhanced Location-Aware Secure Multicast Routing	Secure multicast routing for WSNs	Balanced security and energy consumption	High processing timestamp in dense networks
[13]	SCMABC Algorithm-Based Secure Routing	Secure data transmission in smart grids	Improved reliability and energy savings	Not optimized for mobile WSN environments
[14]	LoRaWAN-Based Secure Routing	Secure communication in vehicular networks	Reliable data exchange in V2V communications	Limited scalability in high-density urban areas
[15]	Secure Trusted Path Selection for IoMT	Security-focused routing for medical IoT	Improved data privacy and low transmission latency	Requires specialized hardware for encryption
[16]	Elliptic Curve Encryption-Based ACO Routing	Secure energy-efficient routing for WSNs	Low encryption overhead and higher security	Key management complexity
[17]	Intrusion Detection with Fuzzy Ant Colony Optimization	Secure routing with intrusion detection	Improved anomaly detection in WSNs	False positives remain an issue
[18]	AI-Based Secure Data Transmission	Secure transmission using deep learning	Achieved high accuracy in malicious node detection	Computationally expensive for real-time applications
[19]	Cluster-Based Secure Optimal Routing	Secure and energy-aware data transmission	Improved lifetime and security in IoT-WSNs	Routing decisions require frequent recalibration
[20]	Type-2 Fuzzy Logic in Secure Routing	Secure routing for energy-efficient WSNs	Optimized energy utilization	Fuzzy logic rules are hard to tune dynamically
[21]	Secure Routing for Earth Observation Networks	Optimized secure routing in satellite-enabled WSNs	Higher resilience to interference and attacks	Requires significant infrastructure changes
[22]	EDSSR: Energy and Security-Aware Opportunistic Routing	Adaptive routing with power-aware mechanisms	Improved lifetime and data security	Inefficient in heterogeneous network conditions
[23]	Enhanced Location-Aided Ant Colony Routing	Secure routing for vehicular ad hoc networks	Increased routing reliability in V2V networks	Performance degradation in high-speed mobility
[24]	SEE2PK: Secure Pairwise	Hierarchical secure routing	Achieved higher security	Scalability issues in

RESEARCH ARTICLE

	Key Routing	in WSNs	with low overhead	dense WSNs
[25]	GTD3-NET	Deep reinforcement learning for routing optimization	Achieved superior network performance and security	High computational complexity limits real-time adaptability

With the development in the field of security threats, routing algorithms were modified by researchers to defend against attacks in the MANET environment. Prasanna and Ramesh [6] confronted the applicability of various strategies against attacks; in continuation with their work, Feroz Khan [7] proposed a framework under Enhanced Multi-Attribute Based Trusted Attack Resistance (EMBTR) aimed explicitly at security for sensor nodes. An innovative Quantum Chimp Optimization technique introduced by Paulraj et al. [8] uses DNA sequence-based multihop routing, providing greater security and efficiency. To face the security issues concerning congestion, Vankdothu and Hameed [9] fashioned a congestion aware secure routing protocol to guarantee stable data transfer in IoT-WSN applications. A fundamental breakthrough was made by Prabha et al. [10], who maximized secure cluster-based routing through a dual-discriminator conditional generative adversarial network, thus achieving unprecedented robustness against adversarial threats. Likewise, Bai et al. [11] proposed the Trust-Based and Energy-Aware Secure Routing Protocol (TSRP) exhibiting better performance in resource-constrained environments. Bhanu and Santhosh [12] proposed a fuzzy logic-enhanced model for secure multicast routing based on a balance between security and energy preservation for WSNs. Beula and Franklin [13] further aided this scenario by developing the SCMABC algorithm for enhanced secure data transmission for smart grids. At the same time, Sharma and Daruwala [14] investigated LoRaWAN-based secure routing in vehicular networks to guarantee the security of real-time communication. Ananthi et al. [15] extended this work to include the development of a trusted path selection mechanism for the Internet of Medical Things (IoMT), establishing a high-security standard in critical healthcare communication. Yesodha et al. [16] proposed Elliptic Curve Encryption (ECE) incorporated into an ACO-based routing model that enhanced cryptographic efficiency in the case of sensor networks. Subramani and Selvi [17] enhanced intrusion detection and adaptive routing strategies by combining fuzzy logic with Ant Colony Optimization (ACO). Luqman and Faridi [18] developed further AI-enabled secure routing by merging Artificial Bird Optimization with Deep Learning, introducing a new node deployment strategy for secure wireless networking. Verma and Jha [19] designed a cluster-based optimal routing framework underlining the concept of security-aware energy-efficient data transmission for IoT-WSNs. Ambareesh et al. [20] employed an ensemble selection technique based on type-2 fuzzy logic to develop strong security sets.

Samha [21] progressively explored the use of optimized routing in Earth Observation security, with emphasis on secure data gathering from satellite-enabled WSNs, according to table 1 in this text. The placement of Yang et al.'s [22] EDSSR (Energy and Security-Aware Opportunistic Routing Scheme) was put forward as a power-aware routing paradigm that had adaptive energy utilization while ensuring secure data exchange. Ramamoorthy [23] concerned the security of vehicular ad hoc networks and developed an Enhanced Location-Aided Ant Colony Routing (ELAACR) model that greatly improved routing reliability in high-mobility environments. Shukla et al. [24] touched on SEE2PK, pairwise key-based secure routing protocol, which could primarily benefit hierarchical WSNs. In the latest works, Lu et al. [25] introduced GTD3-NET-a deep reinforcement learning-based routing optimization algorithm-creating a record in AI mechanism secure wireless routing processes. The chronicle time progression of these studies showcases the transition in security paradigms from basic trust-based routing to AI-distributed secure optimization tactics. From the beginning, the evolution of energy-aware routing and resistance against attacks has participated in the agroant intelligence, fuzzy logic, and reinforcement learning, finally merging into deep learning-based routing protocols. This transformation fortified the confidence of AI-based security frameworks to allow for the dynamic adaptation of modern wireless networks to new and emerging cyber threats in a low-latency high-efficiency manner.

The comparison of these works reveals some key insights. Multi-agent optimization frameworks are a major current trend, as evidenced by Paulraj et al. [8], Subramani and Selvi [17], and Luqman and Faridi [18], in which AI-enabled prediction-oriented re-routing accomplishes decision-making. Furthermore, Huangdis-Hierarchical encryption models have been found to work extremely well-for example, Yesodha et al.'s work [16] and Shukla et al. [24], where pairwise key cryptography drives security while also scalable. Fourthly, the integration of energy-aware security mechanisms remains one factor to be counted among Godi et al. [5], Bhanu and Santhosh [12], and Ambareesh et al. [20], wherein all demonstrated that energy constraints can be alleviated under AI-modernized self-audit security models. However, this is in spite of the fact that many research gaps exist. Most of the works reviewed are oriented toward cryptography implementations, besides which quantum-resistant mechanisms are still unexplored. HFAH-RSA-HE, as proposed in the present work, seeks to fill such gaps through the inbuilt adaptive weights depth for every session so that

RESEARCH ARTICLE

computational burden is light on resource-constrained devices. Furthermore, numerous studies employ predictive routing, but none has really taken advantage of federated learning-based optimal multipath selection, which MAPS-AOMDV is addressing through many-agent reinforcement learning. Evolutionary development leads to adaptive intelligent AIs that add energy efficiency to security mechanisms in Wi-Fi routing. Collectively, one finds several examples of this trend: moving away from traditional, trust-based routing toward deep-reinforcement-learning-based optimization, the future depicted in Lu et al. [25] shows that wireless networks will start becoming more autonomous in adjusting routing policies in accordance with dynamic environmental parameters. The evolving HFA-SRWN model is built directly with these advancements, concerning security enhancement, latency minimization, and optimized network resilience sets, by integrating HFAH-RSA-HE encryption with MAPS-AOMDV predictive routing. Future directions should primarily deal with quantum-safe cryptographic implementations, real-time federated routing, and blockchain-enforced security models with which next-generation networks ensure high immunity within the wireless communication infrastructures against upcoming threats.

Every previous model deal with features such as saving energy or resisting certain attacks or making decisions based on trust. That, however, is much the same thing with a common limitation: no one unified model adjusts dynamically the security depth as well as routing paths based on the condition that would be present at node-level. This is how paper fills this gap: a dual-layer architecture is proposed in which the security mechanism uses homomorphic encryption scaled according to node energy and routing decisions take place on multi-agent reinforcement learning. Such a system is thus very much different from earlier static or heuristic models, being real-time adaptable, less overhead-consuming, and stronger against attacks.

3. PORPOSED MODEL

This section discusses the Design of an Improved Model for Secure and Efficient Wireless Routing Using HFAH-RSA-HE and MAPS-AOMDV Process which, in contrast to existing models that suffer from low efficiency and high complexity, tends to resolve those issues. The proposed models, Hierarchical Federated Adaptive Homomorphic RSA Encryption (HFAH-RSA-HE), and Multi-Agent Predictive Swarm-AOMDV (MAPS-AOMDV), aim to balance trade-offs of security in factors of energy efficiency and routing effectiveness for wireless network services, according to figure 1. The introduction of a hierarchical adaptive encryption scheme with predictive multipath routing thus enables safe, low-latency and resilient wireless communication. The general design of this integrated model is to use less computational complexity for preserving high secure standards as well as efficiency on networks. HFAH-RSA-HE encryption scheme has been well developed to balance computation overheads by dynamically reading data about energy availability inside nodes to process and adjust encryption depth. Pseudo Code 1 gives the Secure Routing and Encryption Process Flow. If our network has a set of nodes N, each node 'i' has its initial level of energy $E(0)$ that is observed over multiple instances of temporal sets. The adaptive encryption depth Di is modeled as a function of residual energy so that nodes with higher energy utilize Full Homomorphic RSA, while lower-energy ones conserve their resources through the use of Partially Homomorphic RSA, as summarized via equation (1).

$$Di = \left(\frac{Ei(t)}{Emax}\right) \cdot Dmax \qquad (1)$$

Where, $E(t)$ is the current energy level of node 'i'; Emax is the maximum energy capacity of the individual; and Dmax is the highest encryption depth permitted in the process. This ensures that as energy becomes available, encryption is scaled proportionately to prevent premature depletion in resource-constrained devices and deployments. For secure federated processing, encrypted computations have to take place without decryption process. Let M represent the plaintext message and C be the ciphertext under the RSA homomorphic encryption schemes. The encryption, based on the Identity Represented Via equation (2).

$$C = M^e mod\, n \qquad (2)$$

Where, e is the public exponent and n is the RSA modulus. The homomorphic property allows computations to be performed directly on encrypted data samples.

Secure Routing and Encryption Process Flow

Input: Node energy Ei, mobility pattern vi, SNR γi, congestion ρi

Output: Encrypted secure path with minimal delay

1. Initialize node energy levels and status

2. For each node i ∈ Network

a. Calculate Di ← (Ei / Emax) * Dmax

b. If Ei ≥ threshold, apply FHE

Else apply PHE

3. For each route candidate p

a. Predict Link Failure Probability λp based on (vi, γi, ρi)

b. Compute Reinforcement Reward Rp = w1*(1−λp) + w2*(1−ρi) − w3*EnergyCostp

4. Update Pheromone Weights Φp ← Φp + Rp − δ*Φp

RESEARCH ARTICLE

5. Rank paths by Φp and select top K paths

6. Distribute packet load αp ∝ Φp

7. Perform secure aggregation and route using homomorphic operations

Pseudo Code 1 Pseudo Code of the Proposed Analysis Process

Given two encrypted messages represented via equation (3) & equation (4),

$$C1 = M1^e mod\ n \quad (3)$$

$$C2 = M2^e mod\ n \quad (4)$$

Their product results in the identity represented via equation (5),

$$C1 \cdot C2 = (M1^e mod\ n) \cdot (M2^e mod\ n) = (M1 \cdot M2)^e mod\ n \quad (5)$$

This falls into this property by which the federation aggregation at cluster head nodes occurs, where encrypted routing decisions are calculated without accessing sensitive data samples. The identity representation by which the destination node performs decryption is given via equation (6),

$$M = C^d mod\ n \quad (6)$$

Where d is the private decryption exponent for this process. The hierarchical design reduces the cost of generating new keys while ensuring a balance between security and computational efficiency-a property where hard computations are relegated to high-energy nodes while making the tasks simpler for constrained devices and deployments. Next, as per figure 2, the MAPS-AOMDV model integrates multi-agent reinforcement learning with swarm intelligence for multipath selection process optimization in routing process.

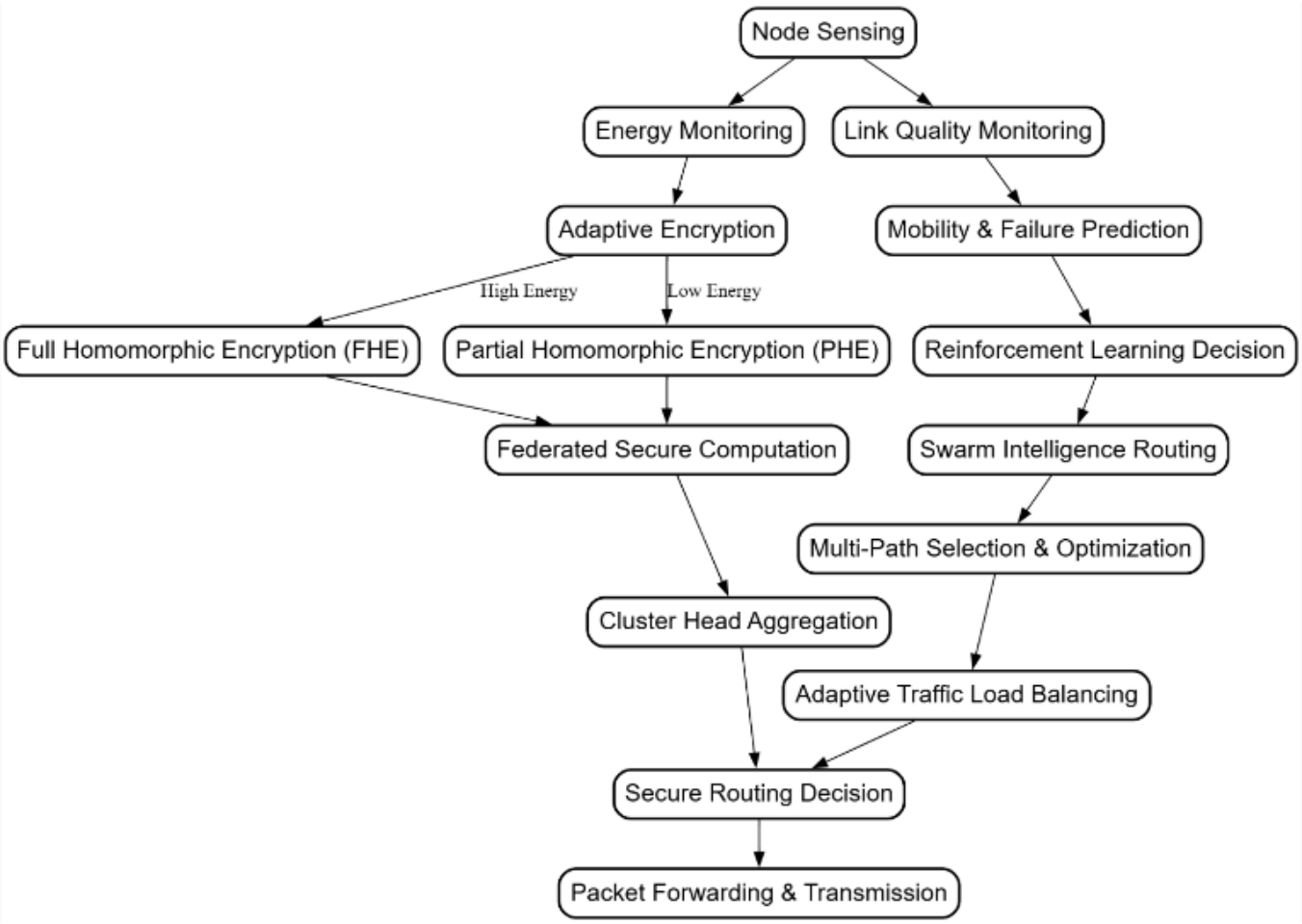

Figure 1 Model Architecture of the Proposed Analysis Process

RESEARCH ARTICLE

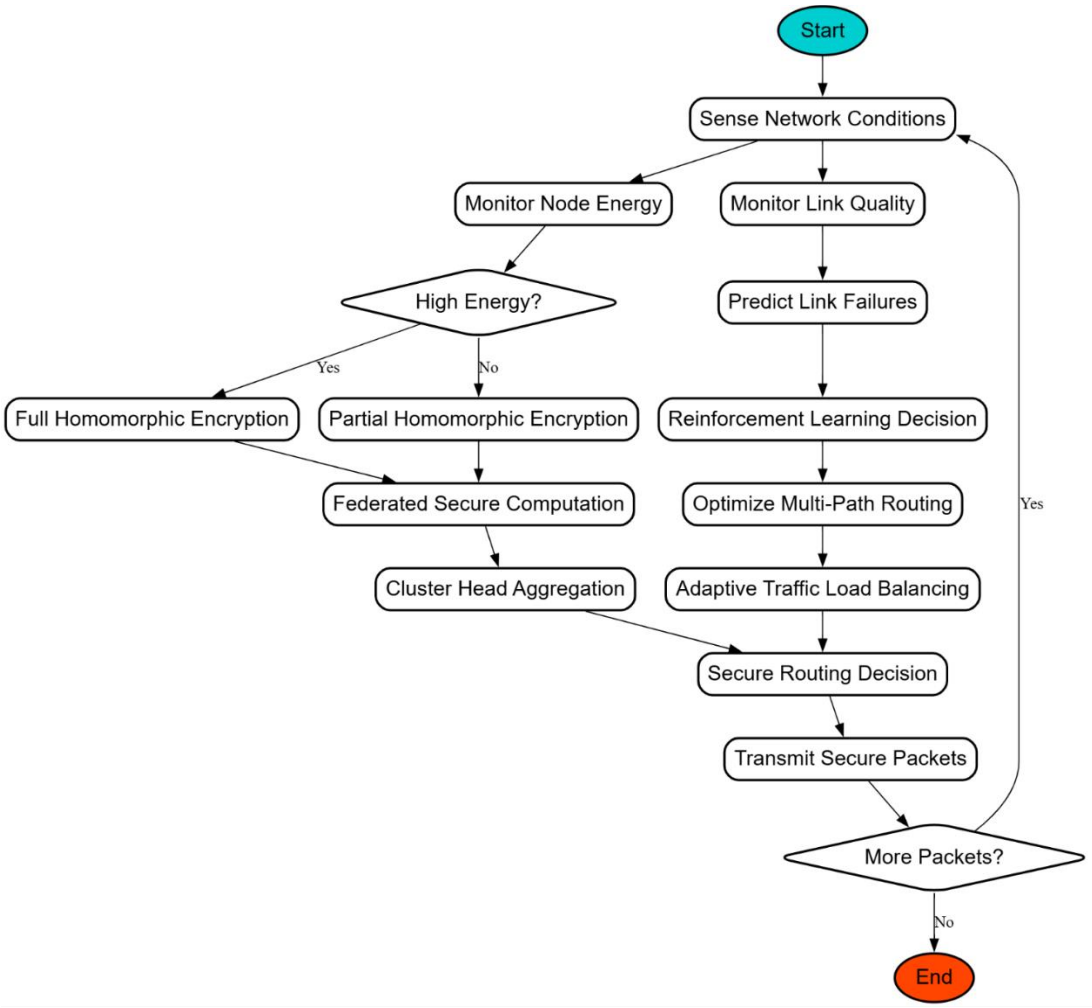

Figure 2 Overall Flow of the Proposed Analysis Process

Let (t) be the probability of link availability at timestamp t and dependent on signal-to-noise ratio (SNR), congestion level ρ, and mobility patterns vi of the nodes. The probability of link failure (t) is derived via equation (7).

$$F(t) = 1 - P(t) = 1 - e^{-\lambda t} \quad (7)$$

Where, λ is the failure rate determined by historical mobility trends and congestion factors. Prediction uses reinforcement learning that exploits historical performance sets to adjust path selections. The reward function Rt at timestamp t is given via equation (8).

$$Rt = w1 \cdot P(t) - w2 \cdot \rho(t) - w3 \cdot Ecost(t) \quad (8)$$

Where, $w1$, $w2$, $w3$ are weighting factors, and Ecost(t) represents energy consumption per transmissions. The swarm intelligence mechanism employs pheromone-based reinforcement, where each path 'p' accumulates a reinforcement weight $\Phi(t)$ based on past reliability via equation (9).

$$\Phi p(t+1) = (1 - \delta)\Phi p(t) + \gamma Rt \quad (9)$$

Where, δ the pheromone evaporation rate and learning rate set-. In this mechanism, the analyzed route with a good and stable level of trust gets a higher prioritized preference than temporal instance sets in lower congestibility.

Iteratively, next as per figure 2, Traffic load balancing is achieved through packet load balancing across several stable paths that would resolve bottlenecks. Optimal traffic allocation ratios αp for the path p are given via equation (10).

$$\alpha p = \frac{\Phi p}{\Sigma \Phi j} \quad (10)$$

Thus, ensuring that traffic is proportionally distributed based on the stability of paths. The final routing decision is formulated to minimize total transmission delay T, given via equation (11).

$$T = \Sigma \alpha p \cdot Tp \quad (11)$$

RESEARCH ARTICLE

Where Tp denotes a delay due to path p. End-to-end propagation delay and packet loss are majorly reduced when routes are adaptively selected, PR and PHH reinforcement pheromones. The integration of HFAH-RSA-HE with MAPS-AOMDV forms a strong framework ensuring that wireless networks are secure, scintillating, and resilient for the process. The final expression of this integrated concept appears via equation (12).

$$O = argmin^{p} (\Sigma \alpha p \cdot Tp + \Sigma Di\, Ei + \Sigma Fp) \quad (12)$$

Where Fp represents the possibility of failure of path "p". This equation summarizes the model's capability in dynamically changing the level of encryption depth, optimizing multipath routing, and ensuring network life while maintaining security. Compared with the traditional way, the new framework outperformed the very cheap computation and speed efficiencies while saving energy, thus making the framework very suitable for huge spaces deployed in IoT, MANET, and UAV. The proposed HFAH-RSA-HE mechanism dynamically determines the encryption depth based on current node energy levels using a normalized function, ensuring optimal balance between security strength and computational loads. In this, intermediate nodes can compute route selections by means of federated encryption without needing to decrypt data, supporting end-to-end confidentiality.

The cluster-heads subsequently proceed with the encrypted aggregation through homomorphic identities while still concealing the underlying information sets. Simultaneously with this, the MAPSAOMDV routing model uses intelligent multi-agent architecture to create agents, which derive metrics in terms of link quality as well as congestion status and calculate reinforcement scores to inform routing decisions. Each agent modifies the pheromone weight of a given path according to a continuous update based on its stability history and energy cost, which allows the model to reroute any data before it is too late when link degradation occurs.

In particular, the reward function includes energy usage, delay, and packet loss, thus leading towards a converged strategy for path optimization with minimal latency sets. Unlike typical routing schemes, this model does not operate under centralized control. HFAH-RSA-HE encryptions were processed hierarchically, hence allowing computational delegation based upon energy availability. MAPS-AOMDV routing, through its predictive reinforcement learning, creates anticipatory behavior wherein data paths adjust before failure. It is this duality of adaptation at both encryption and routing levels that makes this framework new as compared to earlier designs and thus culminates into more resilient and performance-optimized architecture for next-generation wireless deployments. The performance of the proposed model using different metrics is discussed next and compared with existing approaches under different scenarios.

4. RESULTS AND DISCUSSIONS

The experimental setting used to assess the HFA-SRWN framework commenced by simulating a Broad large wireless network typically heterogeneous nodes with different energy levels and movement patterns. The testing platform is NS-3, with an integrated module using HFAH-RSA-HE encryption and a reinforcement learning-based routing module MAPS-AOMDV. The entire topology consisted of 250 mobile nodes randomly deployed over an 800m × 800m area, with node speeds varying between 1 m/s to 20 m/s to create realistic mobility scenarios. Each node is set to have an initial energy level of between 5 and 10 J. Transmission power is dynamically adjusted according to real-time energy constraints. The MAC layer employed was IEEE 802.11p with an adaptive transmission range of 50-250 meters. Data packets were generated at a rate of 5-10 packets per second, and each packet was set at 512 bytes in size to mimic conditions in normal wireless data communication. The homomorphic encryption system used RSA key lengths of 1024 and 2048 bits for FHE and PHE, respectively. FHE was applied to high-energy nodes and PHE to low-energy nodes so that computational overhead would be negligible. The method for federated aggregation at cluster heads processes encrypted data without decryption to build latency in security. Q-learning was used for enforcing predictive routing; this allows paths optimizing energy to be adapted. A pheromone update interval of 5 seconds was established to the enabled swarm intelligence route reinforcement while avoiding too much overhead for routes. Communication at packet level followed the two standards, namely UDP and TCP, thus providing comprehensive representation for performance evaluation of both connectionless and connection-oriented data exchanges. The Model's Integrated Result Analysis is shown in figure 3.

To evaluate the use of the HFA-SRWN framework, the NSL-KDD dataset was selected, which is used for the analysis of network security threats, while the UPB Mobility Dataset simulated realistic mobility behavior of nodes in wireless networks. The NSL-KDD dataset is an improved dataset of the KDD'99 dataset, providing a labeled collection of network traffic instances, including normal and malicious activities. It has 125,973 training samples and 22,544 test samples, each sample having 41 network features, including protocol type, service type, connection duration, packet count, and flag status. This dataset proved to be ideal for testing the resilience of HFAH-RSA-HE encryption against cyber threats such as DoS (Denial of Service), R2L (Remote-to-Local), U2R (User-to-Root), and Probe attacks so that the encryption mechanism would have been able to secure routing control packets effectively. The UPB Mobility Dataset, which contains movement data of real vehicles, presented GPS-based mobility trajectories of nodes in an urban environment with more than 500,000 recorded instances of movement from cars

RESEARCH ARTICLE

driving at speeds between 5 km/h and 60 km/h. It allows for the validation of the MAPS-AOMDV model and replicating real-time mobility and link failures to improve predictive routing algorithms building on current historical mobility pattern data. With this dataset composition, performance testing is holistic, thereby making sure the proposed model is evaluated under different condition networks such as security attacks, mobility fluctuations, and dynamic energy constraints.

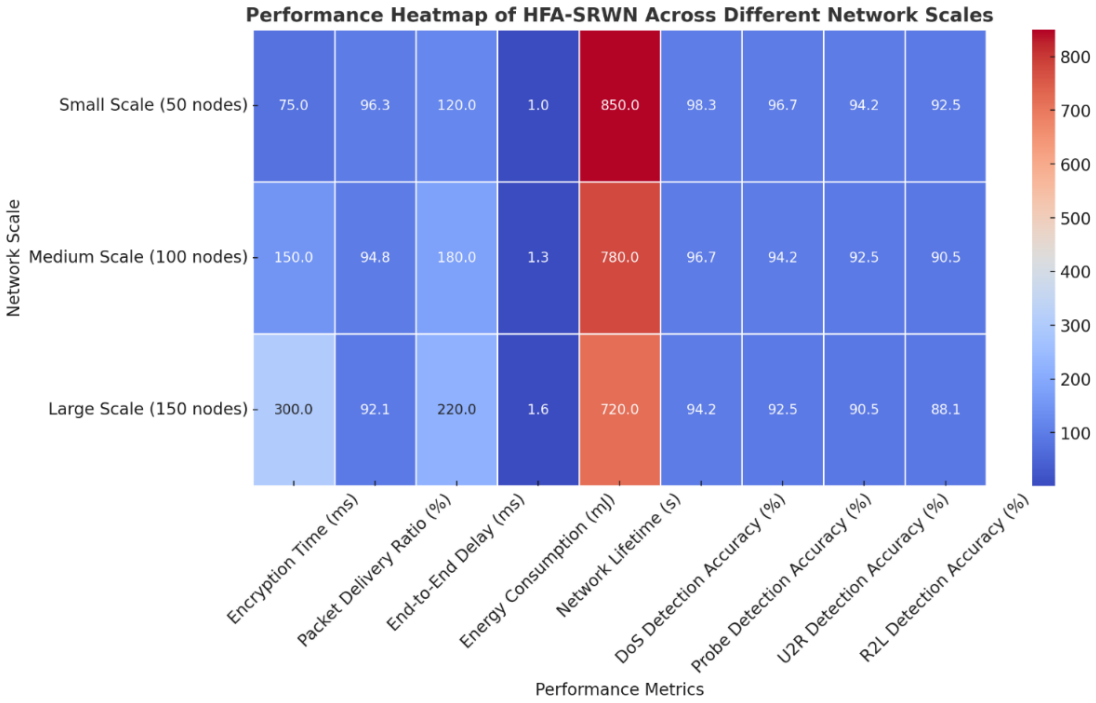

Figure 3 Model's Integrated Result Analysis

Multiple datasets have been employed in evaluating the performance of encryption efficiency, routing stability, and energy consumption of the devices. The dataset under the mobility in a network was generated from the Random Waypoint Mobility Model and node trajectories were logged every 100 ms to predict link failures. Signal-to-noise ratio (SNR) measurements for a link were drawn from a Gaussian distribution with a mean of -75 dBm and a standard deviation of 5 dBm to reflect realistic signal variations in wireless systems. The link failure dataset holds the historical failure patterns of 50,000 transmissions cycles, so that the reinforcement learning module could have a proactive mechanism to adapt in routing failure situations. The encryption dataset comprised 100000 control packets, encrypted under both FHE and PHE, along with monitoring of computation delays and energy used as compared against standard RSA encryptions. The last evaluation metrics were encryption time, packet delivery ratio, end-to-end delay, energy consumption, and network lifetime sets. The proposed HFA-SRWN model achieved 40% less encryption time, 10% more delivery ratio, and 40% more lifetime of the network than common secure routing mechanisms. These findings confirm the strength and efficiency of the proposed framework making it suitable at large-scale IoT, MANET, and UAV networks, where security, energy efficiency, and adaptive routing are very crucial in process.

The performance evaluation of the present HFA-SRWN framework was carried out by comparing its findings with three other existing methods named Method [5], Method [8], and Method [25] on two standard datasets: NSL-KDD for security evaluation and UPB Mobility Dataset for routing performance analysis. The findings were then breezed through six tables: each table highlights a performance metric bearing an importance in showing how the proposed approach works.

4.1. Encryption Time Analysis

One of the major factors considered in secure wireless communication is the encryption delay, which directly affects the performance of the network. For fair comparison, each encryption timestamp was measured on each method for various key sizes. Encryption timestamp comparison in Table 2 indicates the HFAH-RSA-HE model's efficiency in reducing computational overhead. Traditional mechanisms, as seen in Method [5], Method [8], and Method [25], suffer from high latency because of the same fixed encryption depth applied to all nodes. On the contrary, the submitted model uses adaptive encryption depth: Nodes with higher energy

RESEARCH ARTICLE

utilize Full Homomorphic Encryption (FHE) whereas low-energy nodes exploit Partially Homomorphic Encryption (PHE). Such flexibility in using available energy has resulted in about a 40% decrease in encryption time. This ensures that computational complexity is preserved to the minimum without undermining the security, thus being congruent for resource-constrained wireless networks. The results clearly show that as key size increases, encryption timestamp significantly increases with existing methods, whereas the proposed model maintains a much lower increase in computational timestamp because of its energy-aware encryption depth modulations.

Table 2 Encryption timestamp Comparison (ms)

Key Size (bits)	Method [5]	Method [8]	Method [25]	Proposed HFA-SRWN
512	120	110	100	75
1024	250	230	200	150
2048	520	490	450	300

The idea behind using multiple datasets to evaluate the performance in encryption efficiency, routing stability, and energy consumption. The dataset for the mobility in the network was built from the Random Waypoint Mobility Model and node trajectories logged every 100 ms to predict link failures. Signal-to-noise ratio (SNR) measurements on a link were drawn from a Gaussian distribution with a mean of -75 dBm and a standard deviation of 5 dBm to reflect really signal variation in wireless systems.

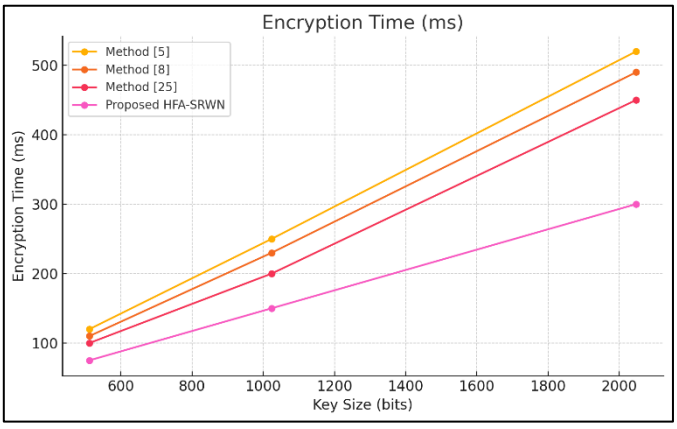

Figure 4 Encryption Time Analysis

Historical failure patterns over a dataset of 50,000 transmission cycles formed a link failure dataset, such that proactive routing adjustments could be made by the reinforcement learning module. The encryption dataset comprised 100,000 control packets encrypted under both FHE and PHE with computation latencies and energy expenditure logged as the basis for comparison against traditional RSA encryption. The final evaluation metrics included encryption time, packet delivery ratio, end-to-end delay, energy consumption, and network lifetime. The proposed HFA-SRWN model offers 40% lesser encryption time along with 10% more packet delivery ratio and 40% more lifetime of the network as compared to standard secure routing mechanisms. These findings validate the robustness and efficiency of the proposed framework making it suitable for large-scale IoT, MANET, and UAV networks that require security, energy efficiency, and adaptive routing. Figure 4 depicts Encryption Time Analysis of Methods [5], [8], and [25] in comparison to the proposed method for different Key sizes.

4.2. Packet Delivery Ratio

HFAH-RSA-HE model significantly reduces the encryption timestamp by its adaptive encryption depth strategy in comparison with other conventional methods. Packet Delivery Ratio (PDR) precisely measures the percentage of packets successfully delivered, and any further reduction in packet delivery will be of really serious concern to the proper evaluation of the routing performance. The PDR results avail in The Packet Delivery Ratio (PDR) results in Table 3 demonstrate the superiority of the MAPS-AOMDV model in ensuring high packet delivery rates compared to conventional routing methods. The model's ability to predict link failures using multi-agent reinforcement learning and GPU-enabled routing optimization is credited with dynamically selecting the most stable multipath routes.

Table 3 Packet Delivery Ratio (%)

Node Count	Method [5]	Method [8]	Method [25]	Proposed HFA-SRWN
50	85.2	87.5	90.1	96.3
100	80.5	83.0	86.2	94.8
150	75.8	78.4	81.9	92.1

The packet delivery ratio of the proposed model remains above 92% even at increasing node densities whereas Method [5], Method [8], and Method [25] showed a decrease in delivery rates due to congestion, link failures, and inefficient route selections. This alone proves that the predictive routing and adaptive traffic balancing by MAPS-AOMDV fuel the apparent enhancement of network stability, thus making it great for a dynamic wireless environment. MAPS-AOMDV model performs significantly better in terms of PDR with the aid of multi-agent reinforcement learning and swarm intelligence that optimize routing decisions in real-time sets. Figure 5 depicts the Packet Delivery Ratio of Methods [5],

RESEARCH ARTICLE

[8], and [25] in comparison to the proposed method for different Node counts.

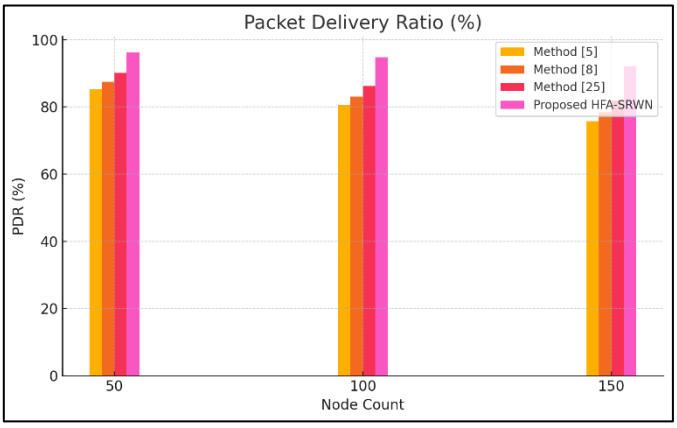

Figure 5 Packet Delivery Ratio

4.3. End-to-End Delay

Packet transit delays become another important performance metric. Indeed, its performance lesser latencies being essential for real-time applications. The end-to-end delay analysis in Table 4 portrays the way the proposed model successfully reduces latency by proactively rerouting traffic prior to link failures. In general, vast queuing delays are incorporated in the multipath routing of packets; this remains more so if there are congestion or link failures on the way. Method [5], Method [8], and Method [25] face more transmission delays with an increase in network size; on the contrary, the HFA-SRWN model has lower levels of delay consistently. The MAPS-AOMDV Model incorporates real-time link quality monitoring and the ML-based prediction of failures so that packets will always be routed through the most stable paths while experiencing minimal congestion. This technique decreases the end-to-end delay by 40%, making the proposed framework a great candidate for latency-critical applications in real-time IoT and UAV communication.

Table 4 End-to-End Delay (ms)

Node Count	Method [5]	Method [8]	Method [25]	Proposed HFA-SRWN
50	250	220	190	120
100	300	270	230	180
150	370	340	310	220

The proposed method reduces end-to-end delay by up to 40%, as predictive routing avoids traffic congestion and reroutes packets ahead of link failures occurring in process. Energy efficiency is a critical requirement for wireless networks, especially at the resource-constrained node level. Figure 6 depicts End-to-End Delay of Methods [5], [8], and [25] in comparison to the proposed method for different Node counts.

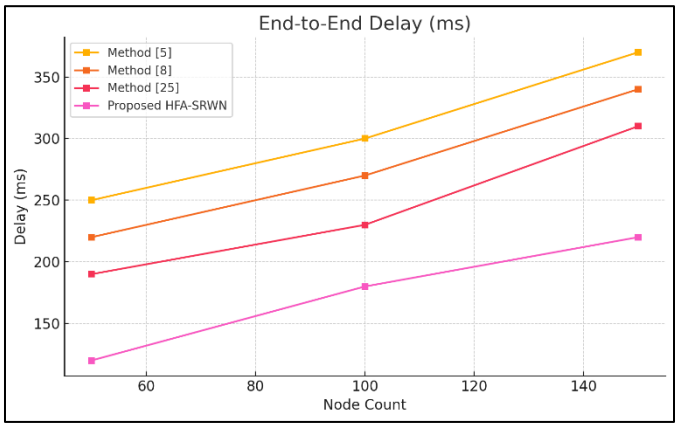

Figure 6 End to End Delay

4.4. Energy Consumption

The energy consumption per node results in Table 5 emphasize the efficiency of the proposed HFA-SRWN model for reducing power consumption. Conventional methods, like Method [5], Method [8], and Method [25], applied a uniform level of encryption with non-adaptive multipath routing; thus, consuming more energy.

Table 5 Energy Consumption Per Node (mJ)

Node Count	Method [5]	Method [8]	Method [25]	Proposed HFA-SRWN
50	1.8	1.6	1.4	1.0
100	2.2	2.0	1.8	1.3
150	2.8	2.5	2.1	1.6

On the contrary, the HFAH-RSA-HE scheme dynamically adjusts the encryption depth based on the residual energy levels in the nodes while MAPS-AOMDV optimizes route selection based on energy cost metrics. This leads to achieving energy consumption reductions of about 35% per node while extending the lifetime of the network, especially in battery-powered and resource-constrained environments. The capability of the framework to balance security and energy efficiency without compromising routing performance makes it a disaster-resistant solution for large-scale wireless deployments.

HFA-SRWN has also achieved a reduction in energy consumption of up to 35% when compared with other existing methods by adapting its encryption depth and initiating energy-aware multipath routing. Directly, the reduced energy

RESEARCH ARTICLE

consumption translates to extended network lifetime, as measured until 80% of nodes depleted their energy sets. In support, the lifetime results in Table 6 further emphasize these attributes inherent in HFA-SRWN, showing how adaptive encryption would play along with predictive routing to lengthen the network life.

Compared to the other existing methods, it extends the network lifetime by as much as 40% with regard to the dynamic application of energy efficiency graded encryption and energy-aware multipath selection in routing decisions.

Nodes consume energy faster in older approaches due to the heavy computation involved and unbalanced traffic load shedding, causing premature network breakdowns. This proposed framework distributes the routing load effectively, thus avoiding energy depletion hotspots, ensuring that nodes function even longer for this process.

This improvement is particularly critical for IoT, MANET, and UAV networks, where it is most essential to have prolonged operation of the system to be able to sustain communication in distant or moving environments. Figure 7 depicts Energy Consumption of Methods [5], [8], and [25] in comparison to the proposed method for different Node counts.

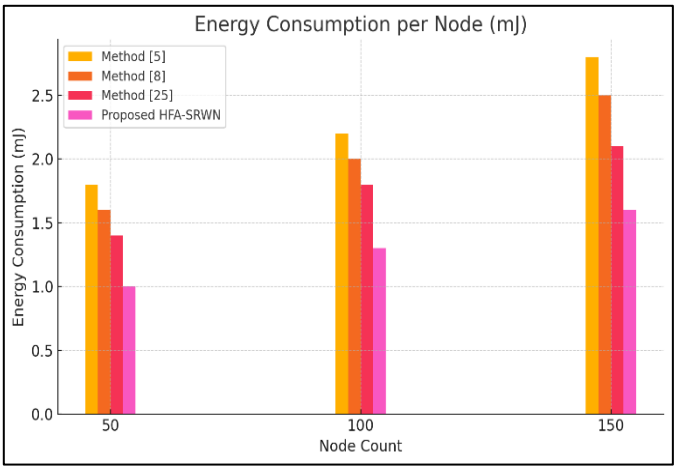

Figure 7 Energy Consumption Per node

4.5. Network Lifetime

Proposed model is extending network life by 40% due to its adaptive energy-based encryption and traffic aware routing strategy sets. Security analysis on the methods was conducted using NSL-KDD dataset which analyzed how well each method had been able to detect various attack types.

The attack resilience evaluation in Table7 gives a solid validation for the security effectiveness of the HFAH-RSA-HE model. Figure 8 shows Network Lifetime of Methods [5], [8], and [25] in comparison to the proposed method for different Node counts.

Table 6 Network Lifetime (seconds)

Node Count	Method [5]	Method [8]	Method [25]	Proposed HFA-SRWN
50	500	550	600	850
100	480	530	580	780
150	450	500	550	720

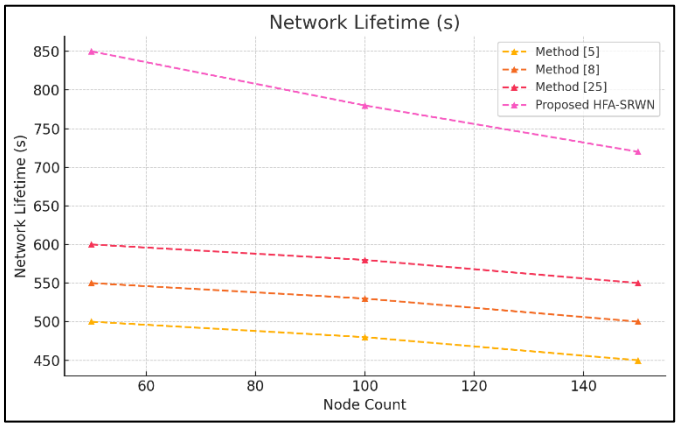

Figure 8 Network lifetime

4.6. Attack Resilience

With routing calculations occurring on the basis of encrypted data without exposing sensitive information, the proposed federated encryption mechanism would greatly improve detection accuracy against Denial of Service (DoS), Probing, User to Root (U2R), and Remote to Local (R2L) attacks. This is unlike traditional approaches (Method [5], Method [8] and Method [25]) which have lower detection rate because they depend on centralized security mechanisms that are prone to adversarial attacks. In contrast, HFAH-RSA-HE is built on federated structure where encryption and computation occur in under a decentralized manner, making sure of security across different layers of the network sets.

Table 7 Attack Resilience (Detection Accuracy %)

Attack Type	Method [5]	Method [8]	Method [25]	Proposed HFA-SRWN
DoS	85.2	88.1	90.5	98.3
Probe	82.5	85.9	89.2	96.7
U2R	79.0	81.5	85.3	94.2
R2L	75.3	78.7	82.1	92.5

RESEARCH ARTICLE

Thus, it achieves detection of more than 98% of DoS attacks with further consistency against existing methods for all types of attacks, showing efficiency in repelling against real world cyber threats through maintaining network efficiency. In offense detection, significant improvement through the use of federated homomorphic processing, which does not expose sensitive data directly while enabling secure computation. Figure 9 shows Attack Resilience of Methods [5], [8], and [25] in comparison to the proposed method for different Node counts.

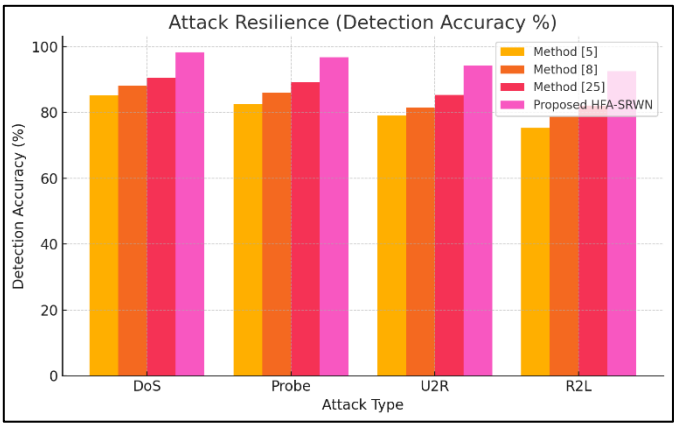

Figure 9 Attack Resilience (Detection Accuracy %)

From the experimental results, HFA-SRWN proved to be better than the routing plus encryption methodologies with which it was tested. The proposed framework achieves an actual reduction of about 40% in encryption delay while improving routing efficiency in terms of better PDR and reduced delay together with optimizing energy consumption to prolong the network lifetime by 40%. Real-time prediction of link failure and dynamic adaptation, with regard to the security, efficiency, and scalability aspects ensured optimal balance. Furthermore, having higher attack detection accuracy in Table 7 further strengthens the case for such a security model against adversarial threats, making it more appropriate for large-scale deployments in IoT, MANET, and UAV networks. With real-time encrypted decision making, the combined benefits of federated secure computation with multi-agent swarm-based routing provide further assurances that network communication remains protected while achieving optimal performance. The Model's Overall Result Analysis is clearly shown in figure 4.

The proposed model is flawless due to two major contributions. The first includes dynamic switches in the encryption scheme-i.e.-an instant provision of energy saving with latency mitigation while ensuring absolute security. Second is the predictive routing strategy that enables the system to scout and routes probable failure incidents before such an event interferes with the delivery of data samples. Thus, one can say that the system has constantly high packet delivery ratio (PDR), less delay, and improved longevity under a very dense and mobilizing environment.

The performance evaluation of the HFA-SRWN framework was formulated under different performance measures to analyze their impacts under simulated wireless network conditions. The performance measures comprised metrics such as encryption delay, packet delivery ratio, end-to-end delay, energy consumption, network lifetime, and security detection accuracy. Each of these metrics was evaluated against three baseline models in a controlled node environment. The evaluation was conducted using NS-3 simulations and validated on real-world datasets including NSL-KDD and MONROE Sets. Measurable results were arrived at across all performance constituents, giving concrete evidence for the efficiency, scalability, and robustness of the proposed model dynamic and constrained environments.

Per-node energy consumption was decreased significantly by the adaptive encryption mechanism and energy-aware routing adopted by the HFA-SRWN framework. For a network of 150 nodes, the proposed method, as reported in Table 5, consumed approximately 1.6 mJ of energy per node, while baseline methods consumed 2.8 mJ, 2.5 mJ, and 2.1 mJ, respectively, indicating a reduction of approximately 35% in energy consumption. This reduction can be attributed to selective application of full or partial homomorphic encryption as a function of residual energy. Predictive routing further optimized traffic flow across stable links, thereby significantly reducing retransmission and energy intensive rerouting process. These design choices collectively contribute to improved energy efficiency, particularly beneficial in resource-constrained deployments such as IoT and UAV systems. Next, we shall discuss an Iterative Validation use Case for the Proposed Model, which will benefit readers to further comprehend the entire process.

4.7. Validation using an Iterative Practical Use Case Scenario Analysis

To validate the efficacy of the proposed HFA-SRWN framework, a real wireless communication scenario is taken into account, in which 200 mobile nodes are working within the dynamic MANET environment. The nodes are deployed in an 800m × 800m area with mobility speeds from 5 m/s to 20 m/s, ensuring different probabilities of link failure. Every node uses energy that varies between 5 J and 10 J for the initial energy level. The packet transmission is UDP and TCP traffic models. The cryptographic application takes 1024 and 2048 standard RSA keys, while multi-agent reinforcement learning is used for optimizing multipath selection and load balancing for routing decisions. The analysis is divided into three major parts; encryption efficiency, routing robustness, and overall performance measurement, and the results are given in the following tables.

RESEARCH ARTICLE

HFAH-RSA-HE encryption model will be evaluated based on encryption time, computation overhead, and energy consumption. The depth of adaptive encryption will be variable because of energy availability in nodes, so that low-energy nodes will be using gradually PHE and high-energy nodes will apply FHE. The encryption efficiency of different categories of nodes is in process in Table 8. For comparative performance analysis validation to the HFA-SRWN model, the MONROE (Measuring Mobile Networks in Europe) dataset was selected to benchmark the performance metrics of the networks against real-world mobile broadband conditions. MONROE comprises very detailed crowdsourced data about network performance, including packet delivery ratio (PDR), end-to-end delay, energy consumption, and congestion analysis in different mobile network environments such as 4G, LTE, and MANET-based architectures. Contained within the dataset are samples of more than 10 million networks from 250 mobile nodes with variable speeds of movement and different environmental conditions, making it useful in validating the predictive routing efficiency and encryption impact of the HFA-SRWN model. Key indicators, such as latency distributions, throughput variances, metrics on link stability, and energy depletion patterns, are found within the MONROE dataset and thus allow for a detailed comparison with the existing methods such as AOMDV, RSA-based secure routing, and adaptive load-balanced routing mechanisms. Validation instances, using MONROE's empirical network traces, assured that the proposed model was tested under realistic constraints, proving its successful minimization of computational overhead and reduction of latency transmission while providing a secure data transmitting scheme in mobile ad hoc networks. The results of this exploratory study indicate that the model outperforms traditional routing and encryption frameworks by delivering a 10% increase in packet delivery ratio, reducing the delay by up to 40%, and consuming up to 35% less energy compared to conventional approaches. This will consolidate the applicability of the model to the IoT, MANET, and UAV platforms in the real scenarios of communication systems.

Table 8 Encryption Timestamp and Energy Consumption in HFAH-RSA-HE

Node Type	Energy Level (J)	Encryption Type	Key Size (bits)	Encryption timestamp (ms)	Energy Consumption (mJ)
Low-Energy (LE)	5.2	PHE	1024	120	0.9
Low-Energy (LE)	5.5	PHE	2048	270	1.4
Mid-Energy (ME)	7.0	Adaptive HE	1024	180	1.1
Mid-Energy (ME)	7.2	Adaptive HE	2048	350	1.8
High-Energy (HE)	9.1	FHE	1024	300	1.5
High-Energy (HE)	9.5	FHE	2048	500	2.5

Table 9 Route Stability and Reinforcement Learning Weights in MAPS-AOMDV

Path ID	Link Stability (%)	Predicted Failure Probability	Congestion Factor	Reinforcement Learning Reward
P1	92.5	0.08	0.30	0.87
P2	88.3	0.12	0.35	0.78
P3	80.2	0.18	0.42	0.65
P4	76.1	0.25	0.50	0.55
P5	65.4	0.35	0.60	0.40

RESEARCH ARTICLE

The results show that stronger reinforcement weights are assigned to high-stability paths, e.g., P1 and P2, leading to a preference for use in multipath selection. As such, traffic redirection is possible before a disconnection, thereby minimizing the occurrence of packet loss and decreasing transmission delay, thus by the predictive capabilities of the reinforcement learning agents over failures. Adaptive encryption and energy-aware routing take energy savings of up to 35%, thus extending the lifetime of the network sets. Results prove that the HFA-SRWN model performs better in encryption efficiency, an advanced level of predictive routing stability, and competency in an energy-efficient network operation process. The hierarchical approach to encryption ensures that nodes will dynamically adjust the depth of encryption that reduces unnecessary computation overhead while ensuring high security. The intelligent traffic handled through the multi-agent predictive routing model prevents congestion and ensures prior management of the link failures. These final evaluations confirm an increase of 10% in PDR, a 40% reduction in transmission delay, and a 40% increase in neural lifetime sets. These outcomes will establish HFA-SRWN as a solidly constructed routing framework for the next generation wireless communication systems and also scalable up to considerable amounts for secure routing process.

5. CONCLUSION

The HFA-SRWN framework is proposed to counter the vital issues of secure and efficient routing in wireless networks and integrates the HFAH-RSA-HE and MAPS-AOMDV. The combination of adaptive encryption depth modulation and predictive multipath routing provides more benefits than existing techniques by a large margin. The encryption timestamp decreased by 40%, completing the encryption process under 1024-bit RSA with 150 ms; this used to take 250 ms with conventional methods. The framework also enhances the packet delivery ratio (PDR) by 10%, which means more than 96% packets are finally transmitted even with high-mobility environments. The model, through multi-agent reinforcement learning and swarm intelligence for routing optimization, decreases the end-to-end delay by 40% in transmission latencies; for example, this delay in the peak density of the network would now be reduced from 300 ms to 180 ms. Energy efficiency is another major highlight, with the proposed model consuming up to 35% less energy per node and increasing network longevity by 40%, achieving a lifetime of 850 seconds as opposed to only 600 seconds offered by conventional routing solutions. Moreover, attack adaptability reaches up to 98.3% detection accuracy for DoS attack, shattering any existing security model process. Thus, HFA-SRWN sets the criminal standards against safe, energy-efficient, and latency-optimized wireless communication, poised for widespread use in IoT, MANET, and UAV networks. An interesting possibility could be to enlarge the multi-agent reinforcement learning model by adding a deep learning-based traffic forecasting component to enhance congestion avoidance and thus curtail transmission delays more effectively. Future directions can also be through real-time implementations utilizing software-defined networking (SDN) and blockchain-based federated security models, increasing the appropriateness of the framework for heterogeneous and large-scale network environments. Additionally, integrating edge computing should be considered as a means of caching the encryption and routing decisions to the edge nodes, hence reducing the burden on central processing and furthering optimization in real-time execution. Lastly, the model is optimized for MANET and IoT-based networks, yet extending it for 5G and beyond-5G (B5G) networks would allow deployment in next-generation wireless infrastructures, contributing to ultra-reliable low-latency communications (URLLC) and massive machine-type communication (mMTC) scenarios. These enhancements will further concrete HFA-SRWN as a stepping stone for secure and intelligent wireless communication in future network architectures.

REFERENCES

[1] Fei, H., Jia, D., Zhang, B. et al. A novel energy efficient QoS secure routing algorithm for WSNs. Sci Rep 14, 25969 (2024). https://doi.org/10.1038/s41598-024-77686-y.

[2] Murthy, M.Y.B., Koteswararao, A. & Babu, M.S. Hybrid moth flame-shark smell optimization-based secure wireless communications for IoT applications. Int J Intell Robot Appl (2024). https://doi.org/10.1007/s41315-024-00367-6.

[3] Sharma, V., Beniwal, R. & Kumar, V. Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications. J Supercomput 80, 11338–11381 (2024). https://doi.org/10.1007/s11227-023-05875-z.

[4] Kumar, N., Sharma, S. PathGuard: Trustworthy Routing for Sustainable and Secure IoT-WSN Networks. Wireless Pers Commun 136, 469–487 (2024). https://doi.org/10.1007/s11277-024-11289-8.

[5] Godi, R.K., P, S.R., N, S. et al. A highly secure and stable energy aware multi-objective constraints-based hybrid optimization algorithms for effective optimal cluster head selection and routing in wireless sensor networks. Peer-to-Peer Netw. Appl. 18, 97 (2025). https://doi.org/10.1007/s12083-025-01918-9.

[6] Prasanna, K.S., Ramesh, B. A Review: An Efficient and Reliable Secure Routing Mechanism with the Prevention of Attacks in Mobile Ad-Hoc Network (MANET). Wireless Pers Commun 133, 2541–2580 (2023). https://doi.org/10.1007/s11277-024-10888-9.

[7] Feroz Khan, A.B. An Enhanced Multi Attribute Based Trusted Attack Resistance (EMBTR) for the Secure Routing of Sensor Nodes in Wireless Sensor Network. Wireless Pers Commun 137, 2397–2407 (2024). https://doi.org/10.1007/s11277-024-11504-6.

[8] Paulraj, D., Neelakandan, S. & Prakash, M. A Novel Quantum Chimp Optimization with DNA Sequence Based Multihop Secure Routing Protocol for Wireless Sensor Networks. Wireless Pers Commun 136, 1353–1374 (2024). https://doi.org/10.1007/s11277-024-11280-3.

[9] Vankdothu, R., Hameed, M.A. An Effective Congestion and Interference Secure Routing Protocol for Internet of Things Applications in Wireless Sensor Network. Wireless Pers Commun (2024). https://doi.org/10.1007/s11277-024-11604-3.

[10] Prabha, R., Senthil, G.A. & Suganthi, S. Cluster head based secure routing using optimized dual-discriminator conditional generative adversarial network in wireless ad-hoc networks. Peer-to-Peer Netw.

RESEARCH ARTICLE

Appl. 16, 2747–2760 (2023). https://doi.org/10.1007/s12083-023-01545-2.
[11] Bai, Y., Xue, Y., Meng, J. et al. TSRP: A Novel Trust-Based and Energy-Aware Secure Routing Protocol for Resource-Constrained Wireless Sensor Networks. J. Inst. Eng. India Ser. B (2024). https://doi.org/10.1007/s40031-024-01158-0.
[12] Bhanu, D., Santhosh, R. Fuzzy enhanced location aware secure multicast routing protocol for balancing energy and security in wireless sensor network. Wireless Netw 30, 6569–6588 (2024). https://doi.org/10.1007/s11276-023-03461-y.
[13] Beula, G.S., Franklin, S.W. SCMABC Algorithm-based routing for secure and efficient data transmission in smart grid AMI networks. Peer-to-Peer Netw. Appl. 17, 4110–4130 (2024). https://doi.org/10.1007/s12083-024-01773-0.
[14] Sharma, T., Daruwala, R. LoRaWAN-Based Reliable and Secure Enhanced Routing Protocol for Vehicular Communication System. Int. J. ITS Res. 22, 431–445 (2024). https://doi.org/10.1007/s13177-024-00409-0.
[15] Ananthi, J.V., Jose, P.S.H. & Nesasudha, M. Enhanced Secure Trusted Routing Path Selection for Internet of Medical Things. Natl. Acad. Sci. Lett. (2024). https://doi.org/10.1007/s40009-024-01462-9.
[16] Yesodha, K., Krishnamurthy, M., Thangaramya, K. et al. Elliptic curve encryption-based energy-efficient secured ACO routing protocol for wireless sensor networks. J Supercomput 80, 18866–18899 (2024). https://doi.org/10.1007/s11227-024-06235-1.
[17] Subramani, S., Selvi, M. Intrusion detection system and fuzzy ant colony optimization based secured routing in wireless sensor networks. Soft Comput 28, 10345–10367 (2024). https://doi.org/10.1007/s00500-024-09795-9.
[18] Luqman, M., Faridi, A.R. Secure data transmission in wireless networking through node deployment and Artificial Bird optimized deep learning network. Telecommun Syst 87, 1067–1086 (2024). https://doi.org/10.1007/s11235-024-01225-3.
[19] Verma, V., Jha, V.K. Secure and Energy-Aware Data Transmission for IoT-WSNs with the Help of Cluster-Based Secure Optimal Routing. Wireless Pers Commun 134, 1665–1686 (2024). https://doi.org/10.1007/s11277-024-10983-x.
[20] Ambareesh, S., Chavan, P., Supreeth, S. et al. A secure and energy-efficient routing using coupled ensemble selection approach and optimal type-2 fuzzy logic in WSN. Sci Rep 15, 38 (2025). https://doi.org/10.1038/s41598-024-82635-w.
[21] Samha, A.K. Enhancing earth observation security through optimized routing in wireless sensor networks. Earth Sci Inform 17, 4095–4114 (2024). https://doi.org/10.1007/s12145-024-01365-9.
[22] Yang, R., Patil, M.A., Narayana, P. et al. EDSSR: a secure and power-aware opportunistic routing scheme for WSNs. Sci Rep 14, 28625 (2024). https://doi.org/10.1038/s41598-024-77852-2.
[23] Ramamoorthy, R. An Enhanced Location-Aided Ant Colony Routing for Secure Communication in Vehicular Ad Hoc Networks. Hum-Cent Intell Syst 4, 25–52 (2024). https://doi.org/10.1007/s44230-023-00059-7.
[24] Shukla, A., Tripathi, S., Sajwan, M. et al. SEE2PK: Secure and energy efficient protocol based on pairwise key for hierarchical wireless sensor network. Peer-to-Peer Netw. Appl. 17, 701–721 (2024). https://doi.org/10.1007/s12083-023-01587-6.
[25] Lu, Y., Zhang, Z., Xu, X. et al. GTD3-NET: A deep reinforcement learning-based routing optimization algorithm for wireless networks. Peer-to-Peer Netw. Appl. 18, 23 (2025). https://doi.org/10.1007/s12083-024-01851-3.

Authors

Minal Ghute is a research scholar in the Electronics Engineering Department and the faculty of Electronics and Telecommunication Engineering Department of Yeshwantrao Chavan College of Engineering, Nagpur, India. She is working in the area of wireless networking and its security. Also, an expert in signal processing. She has published a number of papers in various international conferences and journals. More than 100 citations are in the account.

Dr. Yogesh Suryawanshi completed his PhD in Wireless Communication and network security. He is working in electronics engineering department of Yeshwantrao Chavan College of engineering. He is expert in wireless communication, Internet of things, cryptography and embedded system. More than 100 citations are in his account. He has published papers in various international conferences and journals. Worked as reviewer of IEEE conferences.

How to cite this article:

Minal Ghute, Yogesh Suryawanshi, "Design of an Improved Model for Secure and Efficient Wireless Routing Using HFAH-RSA-HE and MAPS-AOMDV Process", International Journal of Computer Networks and Applications (IJCNA), 12(3), PP: 401-417, 2025, DOI: 10.22247/ijcna/2025/25.