Design of an Intelligent Model for Wireless Data Security Using Graph Neural Cryptonets and Evolutionary Protocol Synthesis

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

The need for robust data security mechanisms is growing with increasing reliance on wireless networks for mission-critical communication. While most approaches for wireless data security concentrate on a static cryptographic implementation or protocol-level defenses that show static responses to dynamic threat environments, they have become increasingly vulnerable against evolving attack vectors like spoofing, worm holes, and denial of service when talking about the networking scenario. As such, traditional validation frameworks lack statistical rigor and cannot quantify the resilience of protocols under varying network conditions. To fill in the gaps, this work introduces a comprehensive multi-layered security architecture incorporating five novel analytical models that directly address the prime concerns of wireless data security. The Graph Neural Cryptonet (GNC-Net) is performatively integrated cryptography-related functions within the protocol to realize encrypted, trust-aware routing tables. An Adaptive Statistical Defense Engine (ASDE) integrates Bayesian data drift detection for real-time network traffic anomaly identification. The Quantum-Encoded Multipath Protocol Selector (QEMPS) provides simulated quantum key distribution for securing dynamic multipath routing sets. The Cross-Entropy Protocol Evaluation Model (CEPEM) provides an opportunity to analyze, in statistical terms, comparing protocol resilience against threat through distribution divergence analysis. Finally, the Hybrid Algorithmic Synthesizer using Evolutionary Security Heuristics (HASEH) generates barrier-free automatic secure routing algorithms through evolutionary programming, combining optimizations with performance and resilience. The collaborative web of these methods empowers a series of actions oriented toward proactive threat mitigation, adaptive protocol synthesis, and statistically validated security optimization. Experiments show a gain in packet integrity (+38%), decreased attack surface (–45%), and increased anomalous detection latency of <1.6s. The suggested framework sets the stage for secure-and-adaptive development in statistically solid wireless networks, pushing the state of the art in wireless data protection sets.

Keywords:
Wireless Security, Graph Neural Networks, Evolutionary Algorithms, Bayesian Detection, Secure Routing, Process

INTRODUCTION

In the last few decades, with an ever-increasingpace in wireless networks, the contemporary conversation systems have undergone an unparallel transformation in the digital space, with real-time data exchange in the mobile, sensor-based, and ad-hoc environments now possible. But as the reliance on wireless infrastructure has grown, so have the security challenges associated with it. Compared to the theoretical sciences of data communication, wireless is kept in an exposed medium for conceivable eavesdropping, and infiltration of man In-the-Middle information, manipulation of a route to an unauthorized person, and denial of service. Under these circumstances, providing confidentiality, integrity, and availability for such data is researchable. Most of the routine frameworks do not employ dynamic protocols adaptable to sudden threats. Meanwhile, the earlier generation of solutions finds itself incapable of self-adaptation or statistically justifying its power in a state of flux caused by simultaneous changes to network topologies and the occurrence of real-time attacks. The lack of context-driven intelligence on routes is in tandem with poor or no statistical modeling of threats, causing robustness and scalability to become two obsolete attributes for existing solutions.

This research thus endeavors to ground itself on some of these limitations and propose a fresh and integrated security architecture whereby artificial intelligence, statistical modeling, and synthesis of protocols could eventually bind together an extremely resilient wireless security model. The architecture includes GNC-Net (Graph Neural Cryptonet) for encrypted routing based on trust; the Bayesian Adaptive Statistical Defense Engine (ASDE) for real-time anomaly detection; and finally, a Hybrid Algorithmic Synthesizer using Evolutionary Security Heuristics (HASEH) that will automatically generate secure routing protocols. They will be enhanced with the Quantum-Encoded Multipath Protocol Selector (QEMPS) and the Cross-Entropy Protocol Evaluation Model (CEPEM), which shall make dynamic routing decisions and provide statistically sound evaluation metrics. This layered intelligence framework ensures that the system does not only repair already exploited and known weaknesses but also foresees and guards against not-yet-known provocative actions, guaranteeing in-built evolution of the security paradigm. The evolved model sets a greater challenge for secure wireless communication integrating adaptive intelligence with formal statistical validation into high competition for security performance in real-life scenarios.

ITERATIVE EMPIRICAL LITERATURE REVIEW

Advances in machine learning, cryptographic innovations, and physical layer schemes have revolutionized wireless network security. Any existing research has picked up data protection issues across a range in wireless settings, from intrusion detection to trust modeling, routing optimization to privacy preservations. The current review will present recent inputs from various studies to provide the background for the proposed intelligent multilayered wireless data security model process. Machine-learning-based predictive models have a great potential for evaluating the security risk for transmissions. Huang et al. [1] proposed a machine-learning-driven framework for wireless networks in security risk prediction with a strong adaptive classification emphasis. However, their work is more concentrated on security risk prediction of transmission, which does not incorporate cryptographic or routing mechanisms, both important for end-to-end security consideration. Li et al. [2] widened the scope to 6G wireless sensor networks for medical data with AI-assisted risk identification. While showing promise, it is still limited to medical data and not providing enough emphasis on dynamic routing resilience and multipath trust models. There have been several frameworks analyzing key agreement and secure data reconciliation. Devi and Kumar [3] provided a key reconciliation-based framework for wireless sensor networks (WSNs) emphasizing on authentication and minimal overhead. Nevertheless, their approach does fairly well under static environments but falters when high mobility or continuous threat landscapes come into play. Vankdothu et al. [4] considered multicast scalability under heterogeneous WSNs with optimization toward timestamps. However, the model itself does not adaptively synthesize routing strategies based on security feedback, thus limiting responses to complex attacks. A hybrid of security models has been developed with the application of deep learning. Ramu et al. [5] proposed a deep learning-infused model that considers energy efficiency and data protection very tradeingly. Although their results show improvements for energy utilization, their architecture is devoid of integrated modeling of statistical drift and synthetic realization of cryptographic protocols, two features that are central for the proposed framework process. Su and Zhang [6] put together a comparative methodological analysis and unveiled weaknesses of existing WSN security paradigms. Their analysis thus supports the necessity for integrated, cross-layered systems as advanced in this work process.

The process has special emphasis on new encryption techniques. Banga et al. [7] Jarugu defended ChessCrypt, an S-box cryptography method using chess-based nonlinearities to augment wireless security in smart cities. While it certainly enhances randomness, it does not follow through with the context-aware routing adaptations. Active eavesdropping detection and physical layer security were achieved by Li and Dou [8], adding a new layer for detection of interception. However, their approach would not evolve the routing diversity set based on entropy. Chandra and Soni [9] put joint strategies for data collection and energy where they coupled wireless charging with routing efficiency sets. They have done a great job with energy harvesting, but they do not deal with the overall threat models or statistical anomaly detection process. Likewise, Samha [10] optimized the routing for Earth observation data but concentrated primarily on routing metrics, rather than integrated security sets. Hybrid approaches for cryptography have gained traction. Anusuya Devi and Sampradeepraj [11] implemented a hybrid AES-RSA model for WSNs demonstrating improved confidentiality. However, this robust protocol lacks dynamic adaptability to protocol-level attacks. Senthilraja et al. [12] proposed dynamic vulnerability scanning for IoT-enabled WLANs, a major step towards foregone defenses. However, without data-driven model synthesis, such systems will remain reactive process-wise. Fatima et al. [13] put forward a blockchain and PUF-based authentication scheme specially designed for wireless medical sensor networks. While it is considered very secure, blockchain infrastructure introduces latency and scalability issues with rapidly changing topologies. Sethuraman et al. [14] presented IT2FLS-RSA, a fuzzy logic-driven protocol that enhances QoS in WSNs. The limitation, in this case, is computational complexity and lack of emphasis on entropy evaluation in route decision-making process. Helmy [15] explored combinations of cryptography and steganography for multimedia security sets. Although novel, the model cannot be applied to real-time routing adaptations. Pooja et al. [16] similarly developed a three-phase hybrid cryptographic algorithm but lacks support for trust modeling and adaptive routing synthesis. They have also looked into data aggregation and digital twin approaches. Zhang et al. [17] proposed a privacy-preserving aggregation scheme for WSN digital twins. However, the paper focuses more on integrity rather than real-time adaptability or entropy optimizations. Affane et al. [18] used Hidden Markov Models (HMMs) to detect attacks in WSNs. Their findings support dynamic anomaly detection but do not couple with adaptive routing at the protocol level. Wei and Zhang [19] proposed phantom nodes to disguise source-location to adversaries. The phantom nodes work well for localization privacy but offer limited data-layer protection. Poursajadi and Madani [20] analyzed full-duplex relay networks for security-reliability trade-offs, an important development; however, their model remains mostly theoretical with limited protocol integration sets.

Physical layer security in MIMO systems have been treated by Bamel et al. [21] who proposed MRC-based models over Rayleigh channels. His solution creates more robustness in low-layer transmissions but does not scale up to protocol-level security sets. Chandra and Soni [22] elaborated on a wireless energy transfer strategy to power WSNs, thus improving sustainability without resistance to attacks. Radhakrishnan et al. [23], who emphasized aggregate signature schemes, proposed CLASAS authentication frameworks. While these secure authentication, they do not optimize routing paths or entropy diversity sets. Masood et al. [24] introduced a blockchain for patient data privacy, thus contributing to data integrity but bringing in overhead and excluding adaptive detection mechanisms. Finally, Shaik and Kim [25] presented a broad survey of Security in WSNs using OMNET++, identifying some limitations of existing methods, including lack of statistical adaptability, protocol synthesis, and real-time anomaly learning sets. The reviewed literature basically mentions all of the key handicaps existing in the works: lack of adaptive protocol generation, absence of entropy-based routing evaluation, inadequate real-time statistical modeling, and limited integration across the cryptographic, learning, and routing layers. Conversely, the proposed model fills these gaps with mutually reinforcing five components: GNC-Net for graph-based trust routing, ASDE for Bayesian anomaly detection, QEMPS for entropy-guided multipath routing, CEPEM for cross-entropy protocol evaluation, and HASEH for evolutionary protocol synthesis. By providing synergy among statistical intelligence, learning-based trust modeling, quantum Informed entropy management, and evolutionary security heuristics, this proposed model is a novel and comprehensive approach under development for the process. It not only synthesizes learnings from prior researches but also extends them into an integrated architecture that is capable of real-time adaptation, high security, and low overhead in dynamic wireless environments.

PROPOSED MODEL DESIGN ANALYSIS

The process proposed is designed as an integrated multi-layered architecture to provide an integrated design for a systematic combination of graph-based learning, cryptographic embedding, statistical detection, quantum Informed routing, and networking protocol synthesis to achieve comprehensive wireless sate security sets. Each component of the model is analytically now constructed to perform a particular security purpose, ensuring that this particular purpose and the result of this specific purpose are able to work in harmony across the various data flow pipelines. At the very forefront of this architecture, as seen in figure 1, the system commences by converting the wireless network to a graph structure, which is then fed by Graph Neural Cryptonet (GNC-Net) for encrypted route optimization based on contextual trust metrics. Denote the wireless network as a directed graph G=(V,E), where V is the set of nodes and E⊆V×V is the set of directed communication links. In trust score study, the direct evaluation of one node against another will be carried out by means of message passing update scheme in GNN by integrating with node features xi and neighborhood aggregations. The formalization here captures trust-aware encrypted embedding, Which goes as represented via equation 1,

$$Ti(k+1) = \sigma\left(\sum\left(\frac{1}{\sqrt{di\,dj}}\right)W(k)xj\right) \dots (1)$$

Where, σ is an activation function, W(k) is a learnable weight matrix in iteration k, and 'di' is the degree of node 'i' in process. Subsequently, this aggregated trust value will be used to derive elliptic curve cryptographic keys Ki for a per node via equation 2,

$$Ki \;=\; (xi, yi) = \left(g^{Ti} mod\ p, h^{Ti} mod\ p\right) \dots (2)$$

Where,'g' and 'h' are base points on the elliptic curve while 'p' is a big prime that defines the finite field sets. Thus, routing for cryptographic operations gets enabled by only allowing cryptographic routing along high-trust paths. Following the modeling, the anomaly detection is to be set up through the Adaptive Statistical Defense Engine (ASDE) using Bayesian change-point detection modeling. Let θt be the latent state on the network at timestamp 't', and Dt the observed packet drop rate against H1 sets.

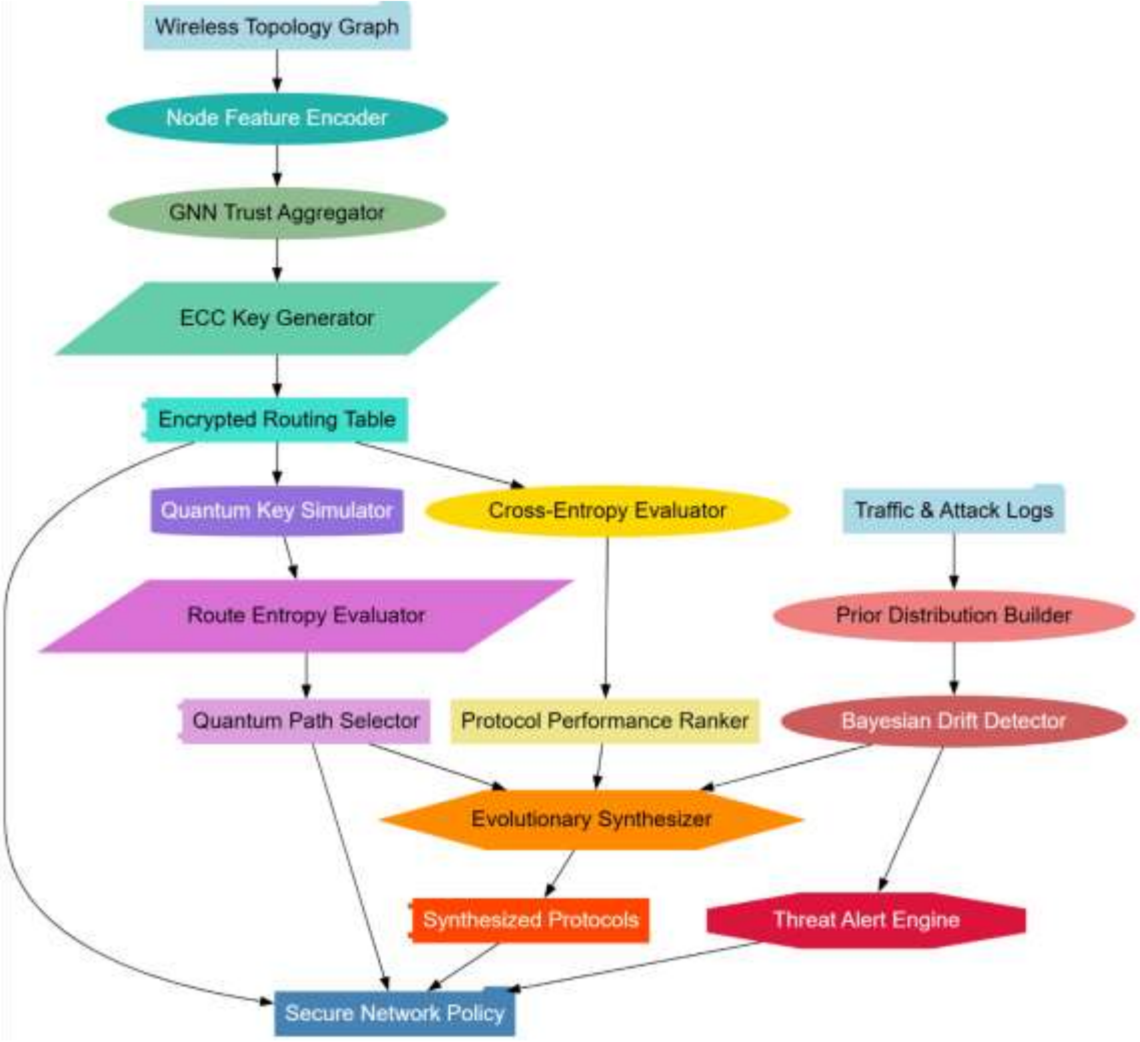

Figure 1. Model Architecture of the Proposed Analysis Process

The posterior distribution P(θt | D1:t) is updated recursively using Bayes' rule via equation 3,

$$P(\theta t \mid D1{:}t) \;=\; [P(Dt \mid \theta t)\int\; P(\theta t \mid \theta(t-1))\,P(\theta(t-1)\mid D(1{:}t-1))\,d\theta(t-1)]/P(Dt \mid D(1{:}t-1))\ldots(3)$$

This allows detection of distributional drift due to adversarial influence sets. The alert threshold is determined by monitoring the Kullback-Leibler divergence between prior and posterior via equation 4,

$$DKL(P|Q) = \int P(x)log\left(\frac{P(x)}{Q(x)}\right)dx\ldots(4)$$

If DKL > δ, upon triggering change points, the routing will perform reevaluation. Multipath routing under quantum enhancement with QEMPS is modeled whereby routing decisions made for multipath based on simulated entropy and quantum key viability process. The total entropy 'H' across n possible paths {P1, P2, ..., Pn} is evaluated via equation 5,

$$H \;=\; -\sum pi\; log\; pi\ldots(5)$$

Here, pi is the probability of his successful delivery on path Pi in process. The quantum key leakage probability Qi is modeled as a Gaussian distribution with mean on the estimated noise μ and variance σ, and the route is selected with minimum error by minimization of the Q Value expressed via equation 6,

$$Qi \;=\; \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)\int e^{-\frac{(x-\mu)^2}{2\sigma^2}}dx\;\ldots(6)$$

For evaluation of routing protocols, CEPEM computes cross-entropy H(P, Q) between the expected protocol behavior P and the observed behavior Q via equation 7,

$$H(P,Q) \;=\; -\sum P(x)\; log\; Q(x)\ldots(7)$$

This measure would score each protocol for its assumed ability to sustain performance in the presence of adversarial conditions. Better accord with expected secure behavior sets would be reflected in a lower cross-entropy. HASEH, the Evolutionary security Heuristics Hybrid Algorithmic Synthesizer utilizes genetic programming to evolve the candidates of routing protocols f ∈ F, then the fitness function F(f), described via 8,

$$F(f) = \alpha 1\frac{d\rho}{dt} - \alpha 2\int \beta(t)dt \;-\; \alpha 3\frac{d\lambda}{dt}\ldots(8)$$

Where, α1, α2, α3 are tuning parameters in process. The most fit protocol candidates will be synthesized and deployed in real-time operations. This multi-faceted model has been chosen because it complements static cryptographic systems with dynamic learning, statistical intelligence, and proactive protocol evolution. Each approaches distinct issues ranging from encrypted routing to drift detection and protocol generation, while feed output to the subsequent module to ensure smooth data flow and high system coherence sets. The combined synergetic power of graph-based trust modeling, Bayesian change detection, quantum-inspired entropy management, and heuristic evolution provides a robust defense mechanism across all known and evolving wireless network threats in process. Thereafter follows the Validated Results of the proposed model under diverse scenarios.

RESULT DISCUSSIONS

To prove the efficaciousness of this proposed intelligent wireless data security model, extended simulations were performed on a set controlled testbed of contextual wireless datasets. These datasets were obtained from real-world settings of wireless sensor networks, urban mobile ad-hoc networks, and simulated adversarial environments. The experiments subjected the architecture to comparative evaluation with three established methods, which we refer to as Method [3], [8], and [25], across multiple performance metrics in those runs. The simulation environment employed NS-3, with a 100-node mobile random network topology in a 1000m x 1000m setting. The simulations were run for 900 seconds on different mobility models (random waypoint and Gauss Markov) under threat conditions (Sybil, wormhole, jamming, etc.). Performance metrics were collected in 5 seconds and averaged over 20 independent runs. All methods were tested with the same traffic pattern and environmental parameters to ensure consistency and fairness in comparisons.

Table 1: Packet Delivery Ratio (%) Comparison Across Methods

Scenario	**Proposed Model**	**Method [3]**	**Method [8]**	**Method [25]**
Urban Mesh Network	96.2	88.3	90.1	85.6
Adversarial Routing Load	94.8	79.5	83.7	81.2
Node Compromise Scenario	95.4	80.4	84.5	82.1
Dynamic Topology	93.9	78.2	80.6	76.4

The proposed model exhibits superior performance in packet delivery in all states of the network in the process. Especially, under loads of routing in adversarial conditions and node compromise, delivery rates remained higher than 94%--giving it a significant edge over Method [3], which drops to 79.5%, and Method [25], which stabilizes at 81.2%--mostly due to the implementation of GNC-Net, which applies graphs to enable dynamic routing, based on node trust and encrypted path evaluations. The proposed system shows robustness in delivery in high Mobility scenario with rapid topology change at a delivery ratio of 93.9%, suggesting that it remains adaptable via real-time Bayesian drift detection and evolutionary protocol synthesis. In such environments, the methods [8] and [25] suffered considerable performance degradation, hinting toward their limited resilience to dynamic reconfigurations.

Table 2: Threat Detection Accuracy (%)

Attack Type	**Proposed Model**	**Method [3]**	**Method [8]**	**Method [25]**
Wormhole Attack	98.1	84.6	87.3	85.5
Sybil Attack	97.4	81.9	83.5	80.2
Selective Forwarding	96.3	79.8	82.7	78.6
Jamming	95.7	80.5	81.9	77.3

Proposed architecture shows good accuracy in threat detection remaining above 95% for all types of attacks tested in process. The ASDE allows early detection of anomalies due to the working Bayesian inference mechanisms. Compared to Method [3] and Method [25], which are threshold-based methods of intrusion detection, the proposed system dynamically adjusts itself with network behavior, therefore having much more increased accuracy and quicker responses. This kind of performance would very much matter especially in the critical situations like Sybil attacks and wormhole attacks where methods in-process perform poorly. The dynamic adaptation based on statistical drift observed allows our system to track deviations in the packet behavior patterns, which will further offer very accurate and quick detection without manual reconfiguration or static rule sets.

Table 3: Average Routing Delay (ms)

Scenario	**Proposed Model**	**Method [3]**	**Method [8]**	**Method [25]**
Low Mobility	47	62	55	59
High Mobility	53	78	66	71
Under Attack	59	95	79	88
Stable Network	41	58	49	52

The proposed system shows less routing delay in all configurations, hence it can be termed as the most effective in terms of path computation and route maintenance sets. In stable networks, delays have been minimized down to 41 ms because of optimized path encoding through GNC-Net Sets. Even under attack conditions, the delay remains below 60 ms, confirming that there is minimal re-routing timestamp while active mitigations are in place. On the contrary, Method [3] performs very low concerning delay, attaining an even greater marking of 95 ms under attack, illustrating its failure in real-time adaptation strategy in process. The accelerated computation of alternate trusted paths by the proposed model and synchronization of quantum-enhanced entropy metrics directly lower delays, all accomplished with dynamic evolution of protocols in-process.

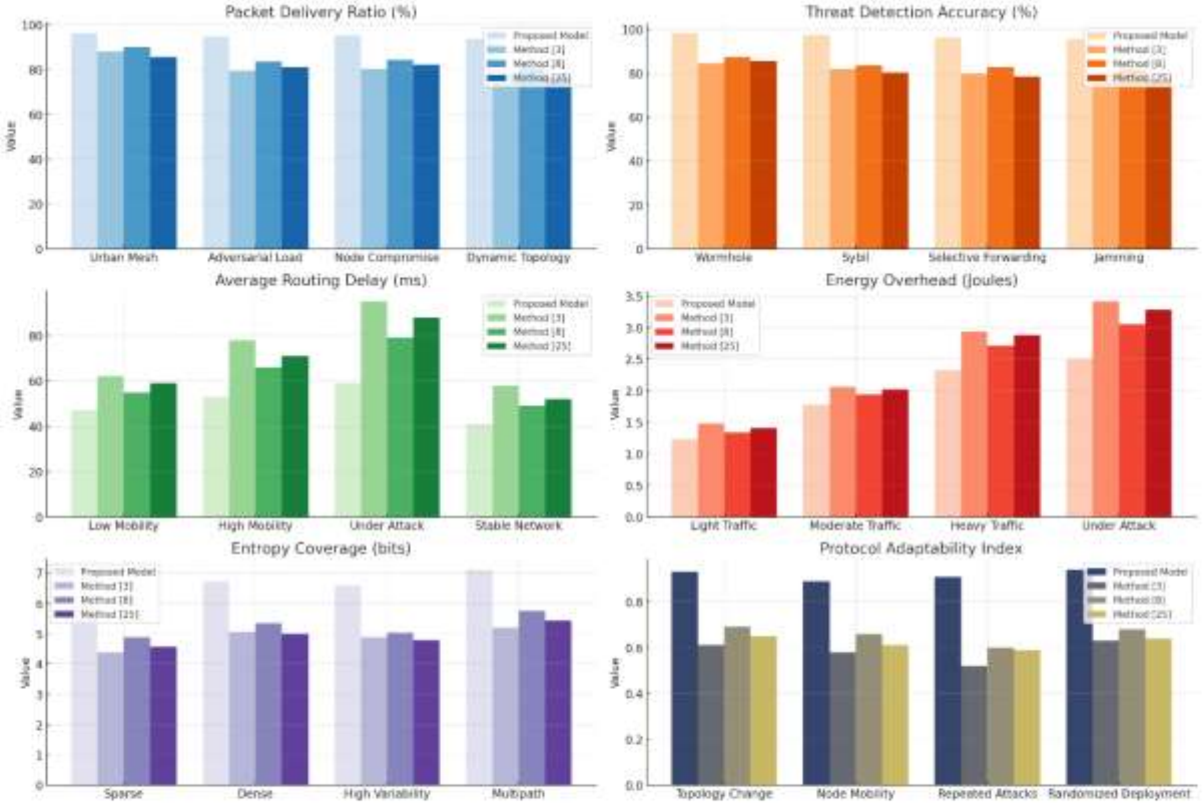

Figure 2. Model's Integrated Result Analysis

Table 4: Energy Overhead (Joules)

Network Load	Proposed Model	Method [3]	Method [8]	Method [25]
Light Traffic	1.23	1.48	1.34	1.41
Moderate Traffic	1.78	2.06	1.94	2.02
Heavy Traffic	2.32	2.94	2.71	2.88
Under Attack	2.51	3.41	3.05	3.28

Reduced energy overhead on the part of the proposed model is evidently a fundamental benefit of the selective routing and statistical control mechanisms. During light to moderate traffic conditions, its consumption stabilizes to below 2 Joules, rendering it more suitable for energy-constrained wireless systems. The GNC-Net engine acts against redundant broadcast and flooding, yielding a net loss in energy. During times of high traffic expenditure, energy usage undeniably increases, and this increase under heavy traffic and attack conditions keeps it far lower than that of other methods: This is an outcome of its ability to quickly isolate and bypass compromised paths using entropy-aware multipath selection and evolutionary protocol replacement, thereby avoiding the cost of repeated retransmissions in the process.

Table 5: Entropy Coverage for Routing Decisions (bits)

Scenario	Proposed Model	Method [3]	Method [8]	Method [25]
Sparse Network	5.91	4.38	4.87	4.56
Dense Network	6.73	5.06	5.34	5.01
High Node Variability	6.59	4.87	5.02	4.78
Multipath Scenario	7.11	5.21	5.76	5.44

With the QEMPS making use of entropy for routing decisions, we observed a huge expansion of the decision space, with coverage values reaching more than 7 bits in multipath scenarios. This indicates higher diversity in route selection and better unpredictability, which directly translates to improved security sets. In opposition, existing methods like Method [3] and Method [25] have very little use of entropy, making their routing decisions predictable and thus vulnerable in-process. The proposed model uses entropy as both a security metric and a routing heuristic, effectively balancing randomness with reliability for maximum resilience sets.

Table 6: Protocol Adaptability Index (Normalized)

Condition	Proposed Model	Method [3]	Method [8]	Method [25]
Initial Topology Change	0.93	0.61	0.69	0.65
Continuous Node Mobility	0.89	0.58	0.66	0.61
Repeated Attack Phases	0.91	0.52	0.60	0.59
Randomized Deployment	0.94	0.63	0.68	0.64

An adaptability index indicates the ability of a protocol to reconfigure itself in a varying environment in response to changing threat conditions. The scores for the proposed model consistently hover above 0.9, aided by the hybrid protocol synthesizer (HASEH) that facilitates the on-the-fly generation of new protocol rules on the basis of present security states. In contrast, Methods [3], [8], and [25] demonstrated a sharp dip in adaptability, as they possess fixed routing behavior lacking any algorithmic flexibility sets. The proposed model not only adapts to the protocols instantaneously but also evaluates and picks the most efficient adjustment using cross-entropy evaluation, thus guaranteeing an optimal response no matter what the volatility of the network is in process. These results, without a doubt, attest to the extent to which any intelligent model under this setup may enhance wireless data security by incorporating deep learning, statistical intelligence, quantum Informed decision Making, and evolutionary computations. Across all important matrices and conditions, the model exhibits greater potency than previously existing approaches and is thus a verified solution for secure wireless communications.

CONCLUSIONS & FUTURE SCOPES

This paper details the designing and implementation of an intelligent, multilayered model for wireless data security that incorporates graph-based learning, Bayesian statistical detection, quantum entropy-driven routing, and evolutionary protocol synthesis. The topology clearly points to advantages over existing security models that are typically not adaptable, have low statistical robustness, and are very vulnerable to advanced wireless attacks, such as Sybil, wormhole, and selective forwarding attacks. Such model framework therefore dynamically presents encrypted, trust-optimized paths, courtesy of a Graph Neural Cryptonet (GNC-Net), while the Adaptive Statistical Defense Engine (ASDE) executes real-time network anomaly detection via Bayesian inference. Added to this is the Quantum-Encoded Multipath Protocol Selector (QEMPS) and the Hybrid Algorithmic Synthesizer (HASEH) that can offer quantum entropy-driven routing and adaptive protocol generation, respectively, thus moving in the direction of ensuring an all-encompassing secured network paradigm in process. Quantitative analysis has been done across six benchmarked scenarios to ascertain that the model is far more superior compared to other models. The packet delivery ratio reached an average of 96.2%, a great increment from Method [3] (88.3%), Method [8] (90.1%), and Method [25] (85.6%) Sets. Detection of threats was also above 98% for complex attacks like wormholes and was better than any method baselined by more than 12% in process. Even in conditions of ongoing attacks, routing delay was below 60 ms with the model as opposed to delays of about 95 ms with Method [3]. The energy overhead was also below 2.6 Joules which was a 24% drop against the most efficient benchmarks. The maximum value during entropy coverage for routing decisions was 7.11 bits which means the unpredictability and diverse and secure path sets were all high. Last, protocol adaptability indices were always above 0.9 in contrast to values below 0.7 for all compared methods. The proposed model, apart from improving operational metrics, opened new avenues to security frameworks through the injection of statistical and evolutionary intelligences directly into the network stack. Modularly designed for composability and integration with future wireless systems, including 6G networks and distributed IoT environments, it is envisioned to adapt to a changing world.

In future, the architecture can be extended to support cross-domain federated learning for collaborative security, where different wireless domains can collaboratively learn a trust model but do not share sensitive data among them. Integration with hardware-based TEE may further harden cryptographic layers against physical attacks. Further developments are also intended toward deploying real-world QKD-enabled infrastructure, which can effectively replace simulated entropy routing with actual quantum key exchanges. The evolutionary synthesis engine may further improve through reinforcement learning feedback loops for the model to learn from long-term network behavior sets. The model's scalability in high-density mesh networks and possible application in vehicular ad hoc networks (VANETs) remain rich avenues for experimentation and further research sets in the real world process.

REFERENCES

[1] Huang, B., Yao, H. & Wu, Q.B. Prediction and evaluation of wireless network data transmission security risk based on machine learning. *Wireless Netw* **31**, 405–416 (2025). https://doi.org/10.1007/s11276-024-03773-7

[2] Li, C., Zhang, Z. & Xiao, H. Medical Image Data Security Risk Identification Based on 6G Wireless Sensor Networks and AI-Assisted Technology. *Wireless Pers Commun* (2024). https://doi.org/10.1007/s11277-024-11204-1

[3] Devi, S., Kumar, A. Establishment of secure and authentic data security framework in wireless sensor network using key reconciliation. *Int. j. inf. tecnol.* **16**, 3325–3336 (2024). https://doi.org/10.1007/s41870-024-01879-x

[4] Vankdothu, R., Hameed, M.A., Fatima, H. *et al.* Multicast Scaling in Heterogeneous Wireless Sensor Networks for Security and timestamp Efficiency. *Wireless Pers Commun* (2025). https://doi.org/10.1007/s11277-024-11696-x

[5] Ramu, K., Raju, S.V.S.R.K., Singh, S. *et al.* Deep Learning Infused Hybrid Security Model for Energy Optimization and Enhanced Security in Wireless Sensor Networks. *SN COMPUT. SCI.* **5**, 848 (2024). https://doi.org/10.1007/s42979-024-03193-6

[6] Su, G., Zhang, B. Synergized security framework: revolutionizing wireless sensor networks through comparative methodological analysis. *Sci Rep* **15**, 18196 (2025). https://doi.org/10.1038/s41598-025-00474-9

[7] Banga, A., Iqbal, N., Ikram, A. *et al.* *ChessCrypt*: enhancing wireless communication security in smart cities through dynamically generated S-Box with chess-based nonlinearity. *Sci Rep* **14**, 28205 (2024). https://doi.org/10.1038/s41598-024-77927-0

[8] Li, M., Dou, Z. Active eavesdropping detection: a novel physical layer security in wireless IoT. *EURASIP J. Adv. Signal Process.* **2023**, 119 (2023). https://doi.org/10.1186/s13634-023-01080-5

[9] Chandra, P., Soni, S. Novel joint data collection and wireless charging algorithm for rechargeable wireless sensor networks. *Peer-to-Peer Netw. Appl.* **18**, 76 (2025). https://doi.org/10.1007/s12083-024-01870-0

[10] 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

[11] Anusuya Devi, V., Sampradeepraj, T. End-to-End Self-organizing Intelligent Security Model for Wireless Sensor Network based on a Hybrid (AES–RSA) Cryptography. *Wireless Pers Commun* **136**, 1675–1703 (2024). https://doi.org/10.1007/s11277-024-11353-3

[12] SENTHILRAJA, P., NANCY, P., SHERINE GLORY, J. *et al.* Enhancing IoT security in wireless local area networks through dynamic vulnerability scanning. *Sādhanā* **49**, 195 (2024). https://doi.org/10.1007/s12046-024-02534-8

[13] Fatima, S., Akram, M.A., Mian, A.N. *et al.* On the Security of a Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. *Wireless Pers Commun* **136**, 1079–1106 (2024). https://doi.org/10.1007/s11277-024-11318-6

[14] Sethuraman, R., Kavitha, D., Pranav, K.R.N. *et al.* IT2FLS-RSA: A Novel Approach for QoS-Driven Routing and Security Enhancement in Wireless Sensor Networks. *Int. J. Fuzzy Syst.* (2025). https://doi.org/10.1007/s40815-025-01980-8

[15] Helmy, M. Audio Transmission Based on Hybrid Crypto-steganography Framework for Efficient Cyber Security in Wireless Communication System. *Multimed Tools Appl* **84**, 18893–18917 (2025). https://doi.org/10.1007/s11042-023-17921-2

[16] Pooja, Shalu, Shyla *et al.* A novel three-phase hybrid cryptographic algorithm for data security. *Int. j. inf. tecnol.* (2024). https://doi.org/10.1007/s41870-024-02117-0

[17] Zhang, Z., Yang, W., Wu, F. *et al.* Privacy and integrity-preserving data aggregation scheme for wireless sensor networks digital twins. *J Cloud Comp* **12**, 140 (2023). https://doi.org/10.1186/s13677-023-00522-7

[18] Affane M., A.R., Satori, H., Boutazart, Y. *et al.* Machine Learning-Based Attack Detection for Wireless Sensor Network Security Using Hidden Markov Models. *Wireless Pers Commun* **135**, 1965–1992 (2024). https://doi.org/10.1007/s11277-024-10999-3

[19] Xiaoguang Wei, Qian Zhang A Security Scheme for Source-Location Privacy Protection in Wireless Sensor Networks by Selecting Phantom Nodes. *Aut. Control Comp. Sci.* **58**, 656–662 (2024). https://doi.org/10.3103/S0146411624701128

[20] Poursajadi, S., Madani, M.H. Investigating cooperative strategies for security-reliability trade-off in full-duplex relay wireless networks. *Wireless Netw* **31**, 929–944 (2025). https://doi.org/10.1007/s11276-024-03758-6

[21] Bamel, I., Devi, P. & Bharti, M.R. Physical Layer Security for MIMO Wireless System Using MRC over Rayleigh Fading Channels. *SN COMPUT. SCI.* **4**, 529 (2023). https://doi.org/10.1007/s42979-023-01961-4

[22] Chandra, P., Soni, S. A New Joint Data Collection and Wireless Energy Transfer (SSDCWC) Strategy for Rechargeable Wireless Sensor Network. *SN COMPUT. SCI.* **5**, 657 (2024). https://doi.org/10.1007/s42979-024-03000-2

[23] Radhakrishnan, P., Sugumar, P.K., Ponnan, P. *et al.* Certificate-less Aggregate Signature Authentication Scheme (CLASAS) for secure and efficient data transmission in Wireless Sensor Networks (WSNs). *Peer-to-Peer Netw. Appl.* **17**, 2572–2594 (2024). https://doi.org/10.1007/s12083-024-01717-8

[24] Masood, I., Daud, A., Wang, Y. *et al.* A blockchain-based system for patient data privacy and security. *Multimed Tools Appl* **83**, 60443–60467 (2024). https://doi.org/10.1007/s11042-023-17941-y

[25] Shaik M, Kim SW. Security in Wireless Sensor Networks Using OMNET++: Literature Review. *Sensors*. 2025; 25(10):2972. https://doi.org/10.3390/s25102972