A Hybrid Framework for Secure Routing Leveraging Multiscale Neuro-Adversarial Validation and Quantum-Driven Pheromone Optimization

Rahul Mahajan, PGDT, Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur, Maharashtra, India
rahulmahajan3102@gmail.com
Srikant V. Sonekar, JD College of Engineering and Management, Nagpur, Maharashtra, India srikantsonekar@gmail.com

Abstract

This study proposes a new combination protocol that will increase the security aspect and efficiency of routing protocols in a network. The suggested system is an effective, intelligent, and adaptive routing system that utilizes Multiscale Neuro-Adversarial Validation (MNAV) and Quantum-Driven Pheromone Optimization (QPO). The framework makes use of adversarial deep learning methodology to verify the directed routes at various scales to detect probed intrusions and prescribe protection against their exploitation. At the same time, QPO, an evolutionary development of classical ant colony optimization with a slightly different ability to use probability-based decisions (quantum-inspired), optimizes the choice of paths. The simulation outcomes indicate a high increase of throughput, latency, and resistance to cyber-attacks in high-level dynamic and decentralized network structures. The combination of neuro-adversarial intelligence and quantum-inspired swarm heuristics represents in itself a viable development in the area of secure network communications.

Keywords: Secure Routing, Quantum-Driven Pheromone Optimization, Neuro-Adversarial Networks, Hybrid Framework, Deep Learning, Network Security, Swarm Intelligence, Multiscale Validation, Quantum Computing, Cyber-Physical Systems.

Introduction:

The digital communication networks are turning out to be complicated in our modern society, and they are widely applied in numerous arenas such as mobile networks, smart cities, the way of defense and Internet of Things (IoT). With the increase in these networks, there are serious concerns characterizing security, speed, and capacity of the network to discover a faster way through which the data can move. The routing system is one of the most significant portions of any network telling how the information will be transferred between two points. In case such routing process is not secure or not efficient enough, the whole system may fail or may easily become the target of attacks.

The conventional routing practices tend to be either rule-based and/or nondynamic; therefore, they lack the capacity to suit new threats or any abrupt transition in the network. Given the increasing instances of cyberattacks and the necessity to use smarter systems, more measures in terms of the use of advanced routing techniques helping to identify threats, be change-resistant but still reliable in terms of communications speed are necessary.

It is to address this issue that our study is suggesting a hybrid framework where we would have two effective technologies combined:

1. Multiscale Neuro-Adversarial Validation (MNAV):

It is a deep learning-based smart system that acts as security checker. It applies the artificial neural networks layers that analyze the traffic in the network to identify anything abnormal or suspicious. It behaves as a watchdog observing the routing procedure and reporting damaging action.

Quantum-Driven Pheromone Optimization (QPO):

The idea behind this approach compares to ant finding food by depositing pheromones. We have a better mechanism to select the path, in our system by employing the concepts of quantum computing and make the process of path selection faster and smarter as well. It assists in determination of an optimal, secure, and most effective path that transmission of data should traverse in the network.

Due to having such two approaches, our framework will not only identify security threats early but also ensure that information travels around the best path possible. This makes the network

secure, fast and reliable even under pressure or attack.

This is because this form of research is expected to develop more intelligent networks that are more secure as artificial intelligence and quantum-inspired optimization strategies are integrated. Our tests indicate that this is a superior combined approach compared to more conventional and to newer versions of routing systems in challenging or dynamic network settings.

Review of literature:

The study by Vasudevan and Ramakrishnan (2020) suggested an AI protocol of secure routing which was specifically designed and implemented in Wireless Sensor Networks and the efficiency of using machine learning to detect and avoid future routing-based attacks was emphasized. Sharma and Rani (2021) addressed the problem and measured the performance of Swarm Intelligence (Swarm Int.) and Quantum-Inspired Swarm Intelligence (QISwarm) ap roaches with an improved mobility in the routing of Mobile Ad-Hoc Networks (MANETs) with better path optimization and environment adaptive decisions. Mishra and Gupta (2019) presented an in-depth survey of different artificial intelligence approaches used to network security, and overall, it was proven that the field of AI supplements real-time threats and adaptive routing processes significantly.

Chaturvedi and Jain (2022) also discussed the future of quantum computing in the field of cybersecurity and how it would transform the secure routing systems in the changing network infrastructure. In Nair and Bhatia (2020) work, a hybrid deep learning model is designed to perform intrusion detection to focus on the better accuracy and faster detection of offensive traffic in network systems. Patel and Desai (2021) offered comparative analysis between AODV and quantum-inspired routing algorithms, which demonstrated the superiority of the latter, with regard to adaptability and path efficiency of the former to the changes in the network conditions.

The introduction of the deep-learning method made a contribution by Jadhav and Wagh (2018), who developed an intrusion detection system based on deep learning, which is able to learn sophisticated patterns of threats and thus drastically minimizes false alarms during the detection process. In the same line of work, Kumbhar and Patil (2020) utilized AI-based methods of secure routing in MANETs and achieved noteworthy gains in packet delivery and insecurity resistance. Singh and Kaur (2019) considered ant colony optimization (ACO) as a routing method in dynamic networks and proved its capability to change performance-real-time adaptability of mobile networks.

Dubey and Sharma (2021) introduced a combination that would boost encryption in data transmission in IoT networks and intelligent routing, a combination of artificial intelligence and cryptography. Dutta and Roy (2019) discussed the implication of quantum cryptography as a budding aspect of network security, by highlighting its significance in further routing operations. Bhosale and Kulkarni (2022) proposed a new smart and safe routing scheme of next-generation networks that meets the requirements of the modern communication system in terms of high speeds and security.

In presetting security in the software-defined networks (SDNs), Ghosh and Sen (2021) have applied deep neural networks, which presented a real-time anomaly detection and dynamic routes alteration. Routines A survey by Sharma and Agarwal (2020) of the quantum inspired routing algorithms concluded that they may perform better than classical models in terms of speed and resilience. Finally, Pandey and Tiwari (2018) modelled and simulated machine learning-based secure routing protocol of unsecure WN that were effective and were experimentally evaluated.

All of these together would indicate the increasing importance of artificial intelligence, deep learning and quantum-inspired optimization in constructing secure, learnable, and high-performance routing systems in modern networks.

Objectives:

- To come up with a safe routing system to allow the application of deep learning algorithms to identify and stop malicious traffic on the network.
- To develop a quantum-inspired pheromone algorithm that will use to know which paths are the most effective and safe to use.
- running 802.11b and 802.11x as a hybrid protocol and comparing the effectiveness of the hybrid in terms of security, speed, and its reliability.

Hypothesis:

- **H_0 (Null Hypothesis):** The convergence of hybrid framework composed of MNAV and QPO does not create substantial improvement in the security / efficiency routing protocols with the available models.
- **H_1 (Alternative Hypothesis):** It is seen that the hybrid framework based on multiscale neuro-adversarial validation and quantum-powered pheromone optimization remarkably improves the security and functionality of network routing as compared with traditional approaches.

Research methodology:

The proposed research is designed and developed based on the network routing design-based and experimental research approach to the development of a hybrid framework of secure and efficient network routing. The whole research process is separated into some stages. To start with, the system architecture included detailed designing of two components Multiscale Neuro-Adversarial Validation (MNAV) and Quantum-Driven Pheromone Optimization (QPO). MNAV module had been created on the basis of deep learning, specifically, adversarial neural networks, to identify malicious or malfunctioning network activity in real-time. Ant colony inspired the QPO module and optimization and is advanced with the quantum computing ideas such that the most appropriate routing arteries should be determined using pheromone-similar notice.

After constructing the framework, simulation environment was developed with the help of a network simulation tool such as NS-3 and Python libraries. Normal and attacking traffic datasets were generated based on synthetic datasets. The hybrid model is then taught and trained in various conditions of networks to determine how good the model will conduct various works in terms of data security, speed of routing and reliability of the path followed.

In order to test the framework, some performance metrics which considered the following parameters, detection ratio, packet delivery ratio, average delay, attack detection rate, and routing overhead were applied. The outcome was compared with the conventional routing techniques such as the AODV and DSR and also compared with some existing AI-based models. In last, statistical tools have been used to estimate the performance gains to prove the efficiency of the suggested system. This approach allowed making sure that the created model could be tested properly and provided actual improvements in what could be offered as alternative solutions.

Analysis of the study:

1. Raw Data Table (Simulated Test Results);

Metric	AODV (Traditional)	AI-Based Model	Proposed Hybrid Model
Packet Delivery Ratio (%)	84.5	91.2	96.8
Avg. Delay (m s)	105	80	65
Routing Overhead (%)	19.5	14.8	11.2
Attack Detection Rate (%)	63.4	81.5	95.3
Throughput (kbps)	325	430	495

Interpretation:

- Packet Delivery Ratio indicates reliability of communication and the Hybrid Model

demonstrates the best one (96.8), the highest.

- In hybrid model, Average Delay (65 m s) is the lowest i.e. faster delivery of data.
- Routing Overhead is the lowest (11.2%) in the hybrid model and this is a sign of good route maintenance.
- They also have better Attack Detection Rate which proves higher security levels in the hybrid model (95.3 percent).
- Its best throughput is 495 kbps, and it has an improved data flow capacity.

2. Comparative Analysis Table (Difference with Proposed Model):

Metric	AODV vs Hybrid	AI vs Hybrid
Packet Delivery Ratio	+12.3%	+5.6%
Avg. Delay	-40 m s	-15 m s
Routing Overhead	-8.3%	-3.6%
Attack Detection Rate	+31.9%	+13.8%
Throughput	+170 kbps	+65 kbps

Interpretation:

- The Hybrid model performs way ahead of AODV in most of the parameters particularly Attack Detection Rate by an increased rate of 31.99 and Throughput of 170 kbps which depicts that it is quite appropriate in secure and high-throughput networks.
- The Hybrid model provides significant advantage even in comparison with the AI-based model, specifically in security (it increases the detection rate by 13.8 percent) and efficiency, (it lowers the delay and overhead).
- The fact that the positive differences are consistent proves that the hybrid approach does lead to evident technical benefits in comparison with current methods.

3. Normalized Performance Score (0– 1 scale)

(Where 1 = best, 0 = worst. Higher PDR, lower delay, lower overhead, higher detection and higher throughput = better)

Metric	AODV	AI Model	Hybrid Model
Packet Delivery Ratio	0.68	0.85	1.00
Avg. Delay (reverse score)	0.50	0.81	1.00
Routing Overhead (rev.)	0.57	0.76	1.00
Attack Detection Rate	0.66	0.86	1.00
Throughput	0.66	0.87	1.00
Average Score	0.61	0.83	1.00

Interpretation:

It can be clearly seen in the normalized scores that Hybrid Model has nearly or even perfect performance as far as all the metrics are concerned.

- The AI-Based Model outperforms the classic AODV, yet it is otherwise inferior to hybrid solution, in delay and security particularly.
- Traditional AODV model proves to be least efficient and least secure in all regards and hence the worst choice module to use when in a threat prevalent environment or in a dynamic environment.

The overall mean performance grade validates the Hybrid model as the most neutral and strong solution of the present network routing demands.

Conclusions Overall Results:

The outcomes of work in question make it clear that the developed Hybrid Framework (the integration of Multiscale Neuro-Adversarial Validation (MNAV) and Quantum-Driven Pheromone Optimization (QPO)) is much more efficient than traditional routing models, as well as AI-based ones. It makes it more secure and quite efficient and data is transferred at a very fast rate through the network. The hybrid model represents significant enhancements to

the packet delivery ratio, minimal increase in the end-to-end delay, minimal routing overhead, and higher attack detection rate, in comparison with the traditional routing approaches such as AODV.

Such a hybrid of the deep learning (intelligent threat detection) and the quantum-inspired optimization (efficient path selection) will mean a powerful and dynamic routing solution applicable in dynamic and decentralized networks like IoT networks, MANETs, and cyber-physical systems. The validity of the hybrid model as a secure communication network is submitted by the experimental outcome and normal performance scores that indicated that the proposed new hybrid model is a more advanced and dependable structure of secure communications.

Future Scope of the study:

Though in simulation the proposed hybrid model produced great outcomes, further research and practical application can be done. In future:

- The real-time implementation networks, where the framework can be applied, are smart city infrastructure, vehicular networks (VANETs) and critical healthcare systems.
- Quantum computing technology innovations could be studied to examine how QPO algorithm will act in it under real conditions.
- A further analysis of energy efficiency can be done, particularly on sensor-based or battery-driven networks.
- They can include adding additional safety layers such as blockchain in and in the name of trust and data secrecy.
- Several ways include; Training the system on more diverse and real-time network traffic data to enhance the system conduct and elastic properties in its wide usage scenarios.

References:

1. Vasudevan, S. K., & Ramakrishnan, M. (2020). AI-Based Secure Routing Protocol for Wireless Sensor Networks. *Journal of Emerging Technologies and Innovative Research (JETIR)*, 7(6), 645– 651.
2. Sharma, A., & Rani, P. (2021). Optimization of Routing in MANET using Swarm Intelligence and Quantum-Inspired Techniques. *International Journal of Computer Applications (IJCA)*, 183(36), 1– 6.
3. Mishra, A., & Gupta, N. (2019). A Survey on Artificial Intelligence Techniques in Network Security. *International Journal of Engineering and Advanced Technology (IJEAT)*, 8(6), 478– 483.
4. Chaturvedi, V., & Jain, S. (2022). Application of Quantum Computing in Cybersecurity: Future of Routing in Networks. *Proceedings of the IEEE International Conference on Smart Technologies (ICST)*, Pune, India, 88– 93.
5. Nair, R., & Bhatia, R. (2020). Hybrid Deep Learning Model for Intrusion Detection in Networks. *Journal of Information and Computational Science*, 10(12), 1132– 1140.
6. Patel, D. B., & Desai, M. M. (2021). A Comparative Study of AODV and Quantum-Inspired Routing in MANETs. *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)*, 9(4), 2263– 2270.
7. Jadhav, R. S., & Wagh, R. B. (2018). **An Effective Intrusion Detection System Using Deep Learning Technique.** *International Journal of Computer Sciences and Engineering (IJCSE)*, 6(9), 681– 686.
8. Kumbhar, M. D., & Patil, S. B. (2020). **Artificial Intelligence Based Secure Routing in Mobile Ad-Hoc Networks (MANETs).** *International Research Journal of Engineering and Technology (IRJET)*, 7(5), 3612– 3616.
9. Singh, R., & Kaur, G. (2019). **Performance Evaluation of Ant Colony Optimization Based Routing in Dynamic Networks.** *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(1), 5324– 5329.

10. Dubey, M., & Sharma, R. (2021). **A Novel Hybrid Approach for Secure Data Transmission Using AI and Cryptography in IoT Networks.** *International Journal of Computer Science and Mobile Computing (IJCSMC)*, 10(5), 88– 95.
11. Dutta, S., & Roy, A. (2019). **Quantum Cryptography: An Emerging Tool for Network Security.** *Proceedings of the All-India Seminar on Emerging Trends in Electronics and Communication (ETEC)*, Institution of Engineers (India), Kolkata.
12. Bhosale, P. N., & Kulkarni, G. B. (2022). **Smart and Secure Routing Protocols for Next-Generation Networks: An AI-Based Framework.** *International Journal of Future Generation Communication and Networking (IJFGCN)*, 15(3), 175– 183.
13. Ghosh, T., & Sen, R. (2021). **Deep Neural Network-Based Security Enhancement in Software-Defined Networks.** *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, 7(2), 322– 328.
14. Sharma, M., & Agarwal, P. (2020). **A Survey on Quantum-Inspired Algorithms in Network Routing.** *Proceedings of the IEEE Conference on Recent Advances in Communication Systems (RACS)*, New Delhi, India, 114– 119.
15. Pandey, P., & Tiwari, N. (2018). **Design and Implementation of Secure Routing Protocols for Wireless Networks Using Machine Learning.** *International Journal of Research and Analytical Reviews (IJRAR)*, 5(3), 20– 28.