

Robust detection of bucket brigade attacks in quantum networks using ascendable quantum non-local neural networks optimized with sharpbelly fish algorithm

L. Thangapalani *

K. Bala [†]

Department of Computer Science and Engineering

School of Computing

Bharath Institute of Science and Technology (BIST)

Chennai 600073

Tamil Nadu

India

Abstract

Quantum communication is based on the laws of quantum mechanics e.g. superposition and no-cloning law to provide highly secure information transmission. In spite of the inherent positive attributes, this is still susceptible to advanced techniques of attack, primarily the Bucket Brigade Attack (BBA). In this attack, the attacker hacks and rereads qubits on a sequence of nodes interacting with each other, effectively damaging transmission without being detected, but emulating the effects of natural channels. Conventional defensive strategies built on such parameters as Quantum Bit Error Rate (QBER) or photon loss are often unable to detect such synchronized anomalies, especially in the case of scaled up multi-hop quantum networks. In order to address this dilemma, intelligent approaches that have the capability to detect hidden non-local relations and learning complex transmission schemes are required. The detection of the accurate attack is performed on an Ascendable Quantum Non-Local Neural Network (AQN-LNN) in the study, and Sharpbelly Fish Optimization algorithm is used to the detection framework and optimize its flexibility

* ORCID-ID: 0000-0003-0418-7725

[†] ORCID-ID: 0009-0003-7623-4778

* E-mail: lthangamsaran@gmail.com (Corresponding Author)

[†] E-mail: bala.hemadharshini@gmail.com

and strength regarding quantum communication security. The proposed approach has an accuracy of 99.9%.

Subject Classification: 68M20, 90B18, 68M10.

Keywords: Ascendable quantum non-local neural network, Sharpbelly fish optimization, Quantum communication, Bucket brigade attack.

I. Introduction

The concept of quantum communication nowadays became paradigm shift in the area of safe information transmission and it is based on the laws of quantum mechanics (superposition, entanglement, and no-cloning) [1]. This is contrary to the classical communication systems, where the security of information is determined by the computational hardness mechanism, quantum communication is made available by the laws of physics [2]. The most common method in this direction is known as Quantum Key Distribution (QKD) where two dishonest individuals are able to share in a common secret key which is unconditionally secure. An action of an opponent that is intended to quantify quantum states causes disturbances that can be quantified and therefore the occurrence of eavesdropping [3].

In spite of these inherent virtues, quantum networks are vulnerable to genuine attacks. One such threat is the Bucket Brigade Attack (BBA), which is an attempt by an adversary to intercept quantum states on intermediate nodes and make an attempt to recombine or relay it. The BBA relies on the multi-hop quantum networks in contrast to the direct intercept-resend attacks that accrue information without detection [4, 5]. This form of attack may impact the privacy of the delivered quantum keys, synchronization, the reliability of communication due to such an attack. Moreover, BBA is highly difficult to use because it can generate the shortcomings of natural transmission, and a user cannot easily distinguish between normal channel noise and adversarial examples [6, 7].

The identification and alleviation of these threats even increase further with the scaling of quantum networks with numerous nodes, numerous repeaters and numerous channels with different characteristics. Sensitivity of classical error analysis to sophisticated interception techniques is not necessarily high enough to be dependent only on QBER or photon loss distributions [8]. Consequently, it leads to the growing necessity to address the smart systems that will identify minor irregularities in the transmission properties and issue the necessary warning concerning the potential intrusion. Such issues need to be solved to safeguard the future generation of quantum communication systems and their stability in practice [9, 10].

The major contributions of this research are;

- Introduced the Ascendable Quantum Non-Local Neural Network to capture hidden non-local correlations in quantum communication data for precise attack detection.
- Applied the Sharpbelly Fish Optimization algorithm to enhance network performance and convergence, maximizing detection accuracy.
- Incorporated critical quantum features, including QBER, polarization mismatch, photon loss, and timing anomalies, to improve sensitivity against BBAs.
- Achieved near-perfect detection performance with 99.9% accuracy, demonstrating robustness across multiple attack strengths and variants.
- Designed a synthetic quantum dataset simulating normal and BBA-affected sessions, enabling systematic evaluation of model effectiveness and feature importance.

A. Manuscript organization

- Section 2: Related works
- Section 3: Proposed Methodology
- Section 4: Results and Discussions
- Section 5: Conclusion

II. Related Works

Several researches were suggested in the literature related to bucket brigade attack detection, among those few recent researches were reviewed in this section.

A stabilized quantum architecture was developed by Tehrani et al. [11] and allowed running hybrid quantum machine learning (HQML) algorithms on actual quantum computers. They proposed hybrid quantum binary classifiers (HQBCs) built on Hoefling decision tree algorithms, which eliminated the need to optimize data processing by processing batches and reduced the number of the shots needed on the real quantum devices than conventional loop-based optimizers. This nature of these algorithms favored the use of online large-scale data streaming on domain generation algorithm (DGA) botnet detection, which further expanded the use of HQML to cybersecurity analytics.

The model of intrusion detection was proposed by Cirillo and Esposito [12] and Gong et al. [21] by applying quantum generative adversarial networks (QGANs) in the context of federated learning. The method used quantum generators and classical discriminators to overcome the computational issues arising in traditional GANs and enhance the capability to model more complex data distributions. The federated hybrid QGAN was evaluated on the NSL-KDD dataset and found to be able to learn benign data distributions, and experiments

were run on a noisy quantum simulator to determine the effect of noise on the detection performance.

Orlandi, Barbierato, and Gatti [13] and Kim and Madhavi [17] found an improvement to financial time series prediction through the use of a quantum Wasserstein generative adversarial network with gradient penalty to generate synthesized data. They reproduced the statistical characteristics of the S&P 500 index and generated data exhibited good fidelity to the original series by measures such as Wasserstein distance, Dynamic Time Warping (DTW) and entropy measures. Moreover, synthetic data sets were used to enhance prediction models and an LSTM based predictor performed better in predicting general trends in the market as well as extreme events.

The Open-Source ROS2 Framework of Outdoor UAV Dataset Generator created by Jarraya et al. [14] and Qi, Wang, and Cui [20] is an inexpensive system that can be used to generate localization datasets of multi-sensors on a UAV. The architecture was ROS2 based on PX4 autopilot, Gazebo simulator and Q Ground Control, which gathered the synchronized information provided by LiDAR, GPS, IMU, camera, and barometer sensors [19]. Additionally, geospatial data from Quantum GIS (QGIS) and Blender were used to generate detailed 3D digital maps, enhancing terrain realism and spatial accuracy for benchmarking learning-based models [22, 24] and sensor fusion techniques.

A. Problem statement

Even the simplest quantum mechanics of quantum communication can offer as much security as is possible, but there are practical challenges which are difficult to solve, posed by advanced adversarial attacks. A multi-hop quantum networks of such BBA is an intimidating threat. An opponent in a BBA interacts with and processes qubits transmitted in the middle of the network, and relaying information to nodes takes action sequentially [16] and over many steps, and an opponent cannot attempt to model the ideal transmission. The main issue with conventional detection mechanisms is that they are based on the implementation of the simple measures such as QBER, and the photon loss especially in large scale networks with repeaters and uneven conditions of channels. This places it in a situation where it is far too hard to see what is real transmission noises [25, 18] and a set of bad interventions. In addition, the optimization of the detection structures in such high-dimensional quantum features space is not as straightforward since non-local complex correlations can be neglected through manual tuning [20, 15]. The challenge therefore that is rapidly gaining pace in intelligent, adaptive detection scheme is the urgent need to detect cleverly the delicate attack patterns with a high degree of trustworthiness and efficiency to offer a quantum communication scheme in real time [23].

III. Proposed Methodology

The research is interested in the vulnerability of quantum communication networks to the state-of-the-art BBA that take advantage of the concept of multi-node transmissions to intercept qubits without any form of suspicion. Conventional approaches (relying solely on the metrics of QBER or photon loss) may be subject to confusing natural-noise in the channel with more cautious adversarial manipulations, particularly when operating on large-scale and multi-hop networks. To address this weakness, the paper presents the AQN-LNN, which has the potential to learn hidden non-local patterns and correlations of the transmitted quantum data. Moreover, the use of SFO algorithm minimizes network parameters, which guarantees maximum adaptability and convergence. Several quantum-level characteristics such as polarization mismatch, timing delays, and photon loss are incorporated in the proposed framework to increase sensitivity of the detection. Validation with a synthetic dataset that is a simulation of a normal and an attack-sessions is carried out. Figure 1, shows the framework of proposed approach.

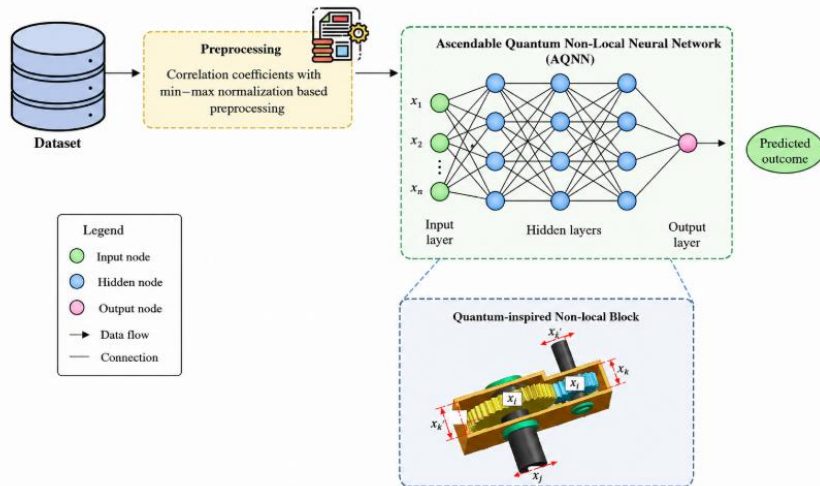


Figure 1
Architecture of the proposed AQNN framework

A. Input Acquisition

In this study a synthetic dataset was created with the help of quantum communication simulator to simulate regular transmissions and to take care of those affected nodes by Bucket Brigade Attacks (BBA). Every session involves qubits interacting via the BB84 protocol and using diverse conditions on the network, such as channel loss, repeater numbers, and decoy states. The dataset records the major quantum and network level characteristics that include:

Quantum Bit Error rate (QBER), Photon polarization mismatch, photon loss ratio, arrival time delays, throughput, entropy and synchronization errors. Each session is characterized as normal (no attack) or being under BBA with the attacker intercepting photons in sequence and retransmitting them to produce anomalies in QBER, polarization states and timing. It has several attack strengths and types (passive, active, partial and distributed) to provide robustness. The data is equal in classes and is divided into training, validation, and testing subsets, which provides a valid basis of deep learning-enabled detection and mitigation of BBA in quantum networks.

B. Correlation coefficients with min-max normalization-based preprocessing

A common normalizing method that transforms data into a fixed scale [1] is min-max normalization. The normalized value for the provider for each criterion is determined using equation (1).

$$A_{\text{norm}}(Q) = \frac{A(Q) - \min(A(Q))}{\max(A(Q)) - \min(A(Q))} \quad (1)$$

$A(Q)$ is the criterion's initial value. The criterion's minimum and maximum values for each provider are $\min(A(Q))$ and $\max(A(Q))$ respectively. In addition to covering all criteria whose results must be comparable, this normalization eliminates any possible distortion brought on by disparate scales or units. The definition of Pearson's correlation coefficient between two criteria is given in equation (2).

$$R = \frac{\sum_{j=1}^n (A_j - \bar{A})(D_j - \bar{D})}{\sqrt{\sum_{j=1}^n (A_j - \bar{A})^2} \sqrt{\sum_{j=1}^n (D_j - \bar{D})^2}} \quad (2).$$

Following correlation analysis, the selected features are normalized to a standard range, often $[0,1]$, using min max normalization.

C. Ascendable Quantum Non-Local Neural Network

AQN-LNN is created to identify fine-grained adversarial attacks on quantum communication by modeling non-local correlations and intricate relations on quantum information. It works in processing some major characteristics like Quantum Bit Error rate, polarization difference, loss of photons and timing variations to determine normal and degraded transmissions. The hierarchical feature learning of the network is made possible by the ascendable architecture, which is more sensitive to small scale disturbances due to Bucket Brigade Attacks. Further, the network is adjusted to the Sharpbelly Fish Optimization to guarantee that the network converges quickly and has high detection rates. In general, AQN-LNN offers a powerful, adaptable, and efficient platform of real-time quantum network security. After that, encrypt this data as equation (3);

$$|\Psi_\Phi\rangle = (\otimes_{h=1}^m A(\lambda_h) K^{\otimes m})|S\rangle \quad (3).$$

The suggested AQN-LNN framework makes use of Variational Quantum Circuits (VQC), which are conceptually adjustable for optimal parameters using a preset cost function. These ansatzes feature three distinct gate R_a configurations that establish interactions between the qubits through capture, ensuring that the quantum state captures the non-local dependence of the data by equation (4).

$$|\psi_1\rangle = M_c(e_0)_{r_0} M_b(\theta_0)_{r_1} M_b(\phi_0)_{r_2} M_a(e_0)_{r_3} |\psi_\Phi\rangle \quad (4)$$

To identify non-local correlations throughout the circuit, these configurations ensure total entanglement between each qubit. Ansatz-0's gateways entangle the qubits in a loop by producing a cyclic pattern. Ansatz-1 uses gates to construct an inverted linear chain, which results in a reversed sequential entangled structure. Ansatz-2 introduces a new, non-linear mixed pattern entanglement method that makes use of the gates. For any connected ansatz, the relevant quantum states are as following equations (5-8):

$$|\psi_2^{[0]}\rangle = R_a(r_1 r_2) R_a(r_2 r_3) R_a(r_3 r_0) |\psi_1\rangle \quad (5)$$

$$|\psi_2^{[1]}\rangle = R_a(r_3 r_2) R_a(r_2 r_1) R_a(r_1 r_0) |\psi_1\rangle \quad (6)$$

$$|\psi_2^{[2]}\rangle = R_a(r_1 r_3) R_a(r_3 r_2) R_a(r_2 r_0) |\psi_1\rangle \quad (7)$$

$$\text{where } R_a = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (8)$$

The most recent gate rotation on each ansatz's qubit 0 can be added to produce the subsequent quantum state by equation (9).

$$|\psi_3^{[x]}\rangle = M_c(a_1)_{r_0} |\psi_2^{[x]}\rangle \quad (9)$$

The gateways and entanglements in that sequence comprise one layer of each ansatz, which the unitary operator additionally depicts as equation (10);

$$O_x(\theta) = |\psi_3^{[x]}\rangle \quad (10)$$

To enhance the model's expression, each layer now contains five parameters that may be applied repeatedly. This results in five parameters that can be trained from the VQC, which is required to ascertain the final state of the circuit by equation (11).

$$|\psi_f\rangle = (O_x(\theta))^L |\psi_\Phi\rangle \quad (11)$$

Measure the remaining qubits in the Pauli-Z computing foundation by evaluating the circuit at a single qubit in the mechanism using the uniqueness function by equation (12).

$$\langle C \rangle = \langle \psi_f | O^\dagger(\theta) R_{r_0} O(\theta) | \psi_f \rangle \quad (12)$$

Its Hermitian adjoint is given by $O^\dagger(\theta)$, and its parameter is the unitary operator θ .

a. *Sharpbelly Fish Optimization*

In order to achieve a balance between exploration and exploitation, SFO is a bio-inspired metaheuristic that imitates the swimming, gathering, evasion, and dispersal behaviors of sharpbelly fish. In order to avoid local optima, the approach uses random swimming, escape, and dispersal to move throughout the search space after starting with a randomly initialized population and assessing fitness to steer motion [15]. After then, it gathers in the best places to take advantage of the greatest solution on the planet. Unless a termination condition, like a maximum number of iterations, is satisfied, iterations continue until the best solution is discovered.

Initialization

The SFO algorithm considers every sharpbelly fish in the search space as a potential solution. The method begins by randomly assigning a population of individuals within the designated bounds. This ensures that each candidate starts the optimization process from a position that is feasible. This can be found using equation (13).

$$B^0 = R(A, R) (U \cdot L) + L \quad (13)$$

B^0 is the starting population, $R(A, R)$ is a matrix of uniformly distributed random numbers, U is the upper and L lower boundaries.

Fitness Function

Equation (14), shows the fitness function

$$\text{Fitness Function} = \text{MIN}(W) \quad (14)$$

where, W is the weight parameter of AQN-LNN, to maximize the accuracy.

Exploitation (Swimming and Gathering)

Swimming is a way for sharpbelly fish to mimic their innate tendency to seek out areas that are high in nutrition. Each fish moves toward the global optimal solution, with speed and fitness having an inverse relationship. The ecological finding that weaker persons are more prone to explore is consistent with this. Equation (15) is used to express it.

$$V_r^{\text{swim}} = e^t \text{rand}() (B_{\text{best}}^t - B_r^t) \quad (15)$$

Exploration (Escape Behavior)

The technique simulates sharpbelly fish's innate propensity to suddenly change course when shocked by simulating their behavior as a stochastic escape

strategy. Random perturbations are applied to individuals with a certain probability in order to imitate this response. While larger probabilities encourage exploration, lower probabilities maintain search stability. It can be found using equation (16).

$$V_r^{\text{disturb}} = \begin{cases} \delta \cdot E(0,1), & \text{if rand} < us, \\ 0, & \text{otherwise.} \end{cases} \quad (16)$$

Position Update

To update its position, each fish in SFO combines swimming, gathering, escaping, and dispersing behaviors. Updating positions while adhering to practical constraints guarantees valid solutions. The top candidate is retained to guide the search during the optimization process, balancing exploration and exploitation by equation (17).

$$B_{\text{best}}^{t+1} = \begin{cases} B_r^{t+1}, & \text{if } s(B_r^{t+1}) < s(B_{\text{best}}^t), \\ B_{\text{best}}^t, & \text{otherwise.} \end{cases} \quad (17)$$

Termination

The SFO method ends when the predefined stopping criterion is satisfied, such as reaching the maximum number of iterations or attaining a certain fitness level. The global best solution found over all iterations is the ultimate optimal solution at termination. The best candidate will be preserved as a result. In order to accomplish efficient optimization, the search process balances exploitation and exploration.

This article proposes a novel detection model that is based on the AQN-LNN that is devoted to estimating some complex and latent relations in the data on quantum transmission. The network exploits various significant properties including QBER, polarization mismatch, and photon loss, and timing errors, which make the network sensitive to the subtle attacks. To further improve the performance, the network parameters are optimized with the algorithm of SFO and thus the network is highly precise and strong to converge. A significant testing that is done is based on a simulated quantum set of problems that are simulating a normal session and BBA-compromised session.

IV. Results and Discussions

The effectiveness of the suggested AQN-LNN framework in detecting Bucket Brigade Attacks in quantum networks is demonstrated by the performance comparison in Table 1. In every way, the AQN-LNN is particularly better than any existing techniques. The quantum bit error rate (QBER) drops dramatically to 0.002, indicating exceptional accuracy in identifying qubit disruptions caused by hostile attacks.

Table 1
QBER, Detection Latency, Photon Loss Rate, Channel Throughput and Polarization Mismatch comparison

Metrics/Techniques	HQML	QGAN	DTW	OS-RFODG	AQN-LNN (Proposed)
Quantum Bit Error Rate (QBER)	0.087	0.065	0.072	0.058	0.002
Detection Latency (ns / qubits)	210	180	195	170	120
Photon Loss Rate (%)	0.18	0.14	0.16	0.12	0.04
Channel Throughput (bps)	0.92e6	1.05e6	1.00e6	1.10e6	1.25e6
Polarization Mismatch (%)	3.5	2.8	3.0	2.6	0.5

Also, compared to HQML, QGAN, DTW, and OS-RFODG, the detection latency is lowered to at least 120 n/qbit, enabling the identification of active attacks more quickly. Additionally, the rate of polarization loss and photon losses is greatly decreased, indicating that the model can accurately monitor quantum states while maintaining signal quality. Furthermore, the channel throughput of 1.25106 bps shows that transmission is effective even when there are attacks. These results support the idea that strong and real-time detection is provided by non-local correlation learning in AQN-LNN and adjusted parameters using the Sharpbelly Fish Optimization. Overall, the architecture ensures that multi-hop quantum communication systems are more secure, dependable, and efficient.

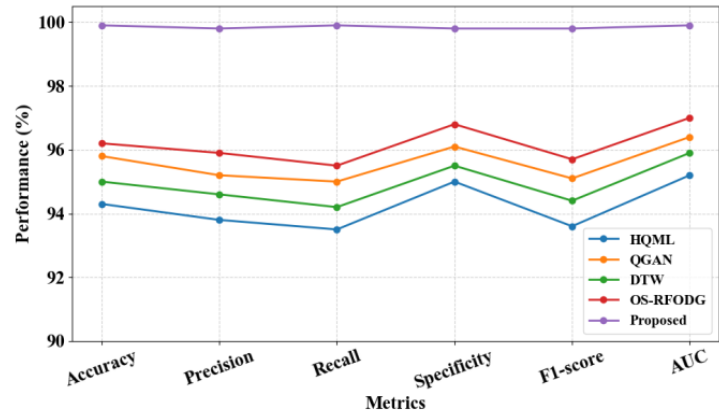


Figure 2
Performance comparison

The proposed AQN-LNN framework is more successful in detecting Bucket Brigade Attacks in quantum networks, according to the comparison of the comparative performance from Figure 2. With an accuracy of 91.9, the model can be considered an almost flawless classifier of attack and normal

sessions, outperforming HQML, QGAN, DTW, and OS-RFODG. The model's capacity to lower false positives while maintaining high detection reliability is confirmed by its precision and F-score of 94.8. Measures of recall and specificity also show similar sensitivity and genuine negative identification, which is crucial for distinguishing between natural channel noise and subtle hostile cases. The robustness of the model can also be justified by the AUC value of 99.9% which indicates great discrimination ability at all thresholds. These findings highlight the significance of combining non-local correlation learning and Sharpbelly Fish Optimization to hyperparameter optimization that improves the accuracy and efficiency of the detection. In general, AQN-LNN framework guarantees that it is highly reliable, low-latency and precise in its detection, which is highly improved compared to current systems of detecting quantum network attacks.

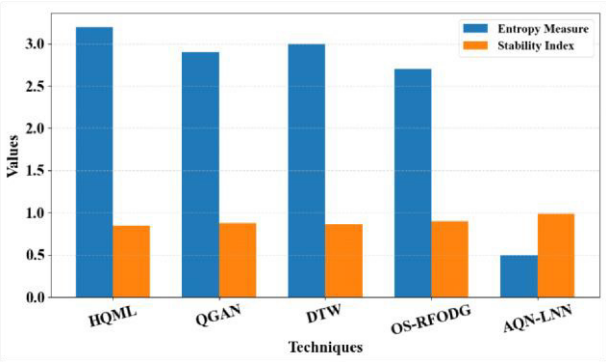


Figure 3
Entropy measure and stability index

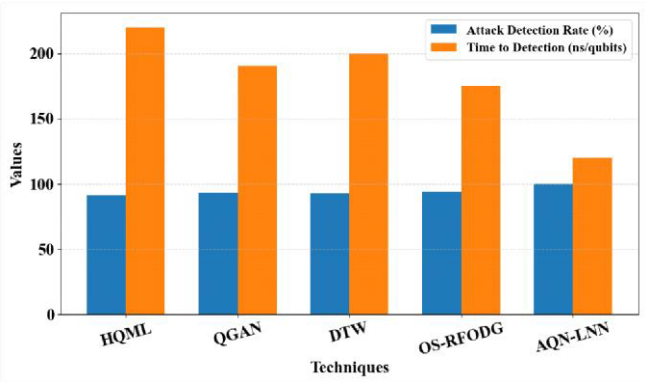


Figure 4
Attack detection rate and time detection comparison

The findings from Figure 3 and 4 prove the efficiency and strength of the suggested AQN-LNN framework in terms of higher evaluation measures. The Entropy Measure is much smaller at 0.5 which means that the model captures a structured pattern in quantum data effectively, reducing randomness and uncertainty, which is brought about by Bucket Brigade Attacks. Attack Detection Rate per Variant stands at 99.9 indicating that the model has the ability to detect the various types of attacks, such as passive, active, partial and distributed BBAs. Also, the shortest response time of 120 ns/qubit is the lowest, which is fast enough to respond in real-time during quantum network security. Stability Index of 0.99 explains the repetition of the experiment and the presence of different network conditions are also reliable and consistent. AQN-LNN is the best pattern recognition, adaptability and robustness in comparison with HQML, QGAN, DTW, and OS-RFODG which justify the benefits of combining non-local correlation learning and Sharpbelly Fish Optimization to detect quantum network attacks.

Table 2
Ablation study

Configuration	Features Used	Optimization	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	AUC (%)
C1: Full Model	All features (QBER, polarization mismatch, photon loss, timing)	SFO	99.9	99.8	99.9	99.8	99.9
C2: No Timing Features	All except arrival delay & sync errors	SFO	98.7	98.4	98.6	98.5	98.8
C3: No Polarization Features	All except polarization mismatch	SFO	98.1	97.8	98.0	97.9	98.3
C4: No Optimization	All features	None (default weights)	98.5	98.2	98.4	98.3	98.6
C5: Minimal Features	QBER + photon loss only	SFO	95.2	94.9	95.0	94.9	95.5

The ablation study in Table 2, explores the role of important elements of the proposed AQN-LNN framework being optimized with the help of SFO. The entire model (C1), with all quantum and network-level capabilities and SFO optimization) gives a remarkable 99.9% accuracy, indicating the usefulness of

when either timing features (C2) or polarization mismatch features (C3) are removed, which implies that these features are very important in the detection of subtle anomalies due to Bucket Brigade Attacks. The effect of optimization (C4) being switched off also brings a tangible decrease, which underscores the role of SFO in tuning network parameters to the highest level. Lastly, the lowest of the features (C5) demonstrates the lowest metrics, and this proves that the use of QBER and photon loss exclusively alone is not sufficient to achieve strong detection. On the whole, this ablation confirms that the totality of features and optimization is the key to the near-perfect attack detection in quantum networks.

V. Conclusion

This paper provides a good model of identifying a Bucket Brigade Attack in quantum networks through AQN-LNN trained with a Sharpbelly Fish Optimization. The proposed model shows excellent results in a variety of measurements and shows a 99.9 percent accuracy, a smaller Quantum Bit Error rate (0.002), a low detection latency (120 ns/qubit) and low photon loss (0.04 percent) and a higher channel throughput ($1.25 \cdot 10^6$ bps). Those findings demonstrate that the framework can effectively detect subtle adversarial manipulations and maintain the integrity of communication, which is superior to the current methods like HQML, QGAN, DTW, and OS-RFODG. To apply the framework to real-world quantum network testbeds in the future, it is possible to extend the work to dynamic multi-node topologies and a wide range of attack strategies to test the robustness in real-world conditions. Combining online learning methods would also perhaps allow adaptive detection to emerging threats. Other future directions might involve hybrid quantum-classical neural networks and architectures, as well as hardware-efficient designs, which will enable quantum communication networks to be secure and scalable.

References

- [1] Z. Zhang, Y.-J. Wang, P. Wang, R.-Z. Zhao, X.-Y. Yang, Z.-A. Zhao, T.-L. Wang, H.-F. Zhang, Z.-F. Li, Y. Wu, H.-R. Tao, L.-L. Guo, L. Du, C. Zhang, Z.-L. Jia, W.-C. Kong, Z.-Z. Zhang, X.-X. Song, Y.-C. Wu, Z.-Y. Chen, P. Duan, and G.-P. Guo, "Demonstrating Coherent Quantum Routers for Bucket-Brigade Quantum Random Access Memory on a Superconducting Processor," *arXiv preprint*, arXiv:2505.13958 (May 20, 2025).
- [2] P. Mukhopadhyay, "A quantum random access memory (QRAM) using a polynomial encoding of binary strings," *Sci. Rep.*, vol. 15, no. 1, Art. no. 11002 (Mar. 31, 2025), doi: 10.1038/s41598-025-95283-5.

- [3] O. Di Matteo, V. Gheorghiu, and M. Mosca, "Fault-tolerant resource estimation of quantum random-access memories," *IEEE Trans. Quantum Eng.*, vol. 1, pp. 1–13 (Jan. 17, 2020), doi: 10.1109/TQE.2020.2965803.
- [4] D. Kim, S. Heng, S. Heng, and Y. Han, "Maximizing the Yield of Bucket Brigade Quantum Random Access Memory using Redundancy Repair," arXiv:2312.17483, (Dec. 29, 2023).
- [5] F. Shen, Y. Ji, D. Xiang, Y. Wang, K. Wang, C. Zhang, A. Zhang, Y. Zou, Y. Gao, Z. Cui, G. Liu, J. Yang, Y. Han, J. Deng, A. Wang, Z. Zhang, H. Li, Q. Guo, P. Zhang, C. Song, L. Lu, Z. Wang, and J. Yin, "Experimental Realization of the Bucket-Brigade Quantum Random Access Memory," arXiv preprint arXiv:2506.16682 (Jun. 2025).
- [6] R. Asaka, K. Sakai, and R. Yahagi, "Quantum random access memory via quantum walk," *Quantum Sci. Technol.*, vol. 6, no. 3, Art. no. 035004 (2021), doi: 10.1088/2058-9565/abf484.
- [7] Y.-J. Wang, T.-P. Sun, X.-N. Zhuang, X.-F. Xu, H.-Y. Liu, C. Xue, Y.-C. Wu, Z.-Y. Chen, and G.-P. Guo, "Efficient Classical Simulation of the Quantum Random Access Memory," *arXiv preprint arXiv:2503.13832* (Mar. 18, 2025).
- [8] P. Mukhopadhyay, "A quantum random access memory (QRAM) using a polynomial encoding of binary strings," *Sci. Rep.*, vol. 15, Art. no. 11002 (Mar. 2025), doi: 10.1038/s41598-025-95283-5.
- [9] Z.-Y. Chen, C. Xue, Y.-J. Wang, T.-P. Sun, H.-Y. Liu, X.-N. Zhuang, M.-H. Dou, T.-R. Zou, Y. Fang, Y.-C. Wu, and G.-P. Guo, "Efficient and error-resilient data access protocols for a limited-sized quantum random access memory," *arXiv preprint arXiv:2303.05207* (2023).
- [10] L. Spyridopoulos, D. Ntalaperas, and N. Konofaos, "Qutrit control for bucket brigade RAM using transmon systems," *Applied Sciences*, vol. 15, no. 7, Art. no. 3950 (Apr. 2025), doi: 10.3390/app15073950.
- [11] M. G. Tehrani, E. Sultanow, W. J. Buchanan, M. Amir, A. Jeschke, M. Houmani, R. Chow, and M. Lemoudden, "Stabilized quantum-enhanced SIEM architecture and speed-up through Hoeffding tree algorithms enable quantum cybersecurity analytics in botnet detection," *Scientific Reports*, vol. 14, no. 1, Art. no. 1732 (Jan. 19, 2024), doi: 10.1038/s41598-024-51941-8.
- [12] F. Cirillo and C. Esposito, "Intrusion detection using quantum generative adversarial networks: A federated approach with noisy simu-

- lators," in *IET Space and Communications Conference 2025*, vol. 2025, pp. 31–35 (2025), doi: 10.1049/icp.2025.2226.
- [13] F. Orlandi, E. Barbierato, and A. Gatti, "Enhancing financial time series prediction with quantum-enhanced synthetic data generation: A case study on the S&P 500 using a quantum Wasserstein generative adversarial network approach with a gradient penalty," *Electronics*, vol. 13, no. 11, Art. no. 2158 (Jun. 2024), doi: 10.3390/electronics13112158.
- [14] I. Jarraya, M. Abdelkader, K. Gabr, M. B. Kadri, F. Alahmed, W. Boulila, and A. Koubaa, "OS-RFODG: Open-source ROS2 framework for outdoor UAV dataset generation," *Results in Engineering*, vol. 27, Art. no. 106613 (Aug. 2025), doi: 10.1016/j.rineng.2025.106613.
- [15] J. Liu, R. Wang, Y. Deng, X. Huang, and Z. Li, "Sharpbelly fish optimization algorithm: A bio-inspired metaheuristic for complex engineering," *Biomimetics*, vol. 10, no. 7, Art. no. 445 (Jul. 2025), doi: 10.3390/biomimetics10070445.
- [16] M. Hdaib, S. Rajasegarar, and L. Pan, "Quantum deep learning-based anomaly detection for enhanced network security," *Quantum Machine Intelligence*, vol. 6, Art. no. 26 (2024), doi: 10.1007/s42484-024-00163-2.
- [17] T. H. Kim and S. Madhavi, "Quantum intrusion detection system using outlier analysis," *Scientific Reports*, vol. 14, Art. no. 27114 (2024), doi: 10.1038/s41598-024-78389-0.
- [18] E. I. Elsedimy, H. Elhadidy, and S. M. M. Abohashish, "A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer," *Cluster Computing*, vol. 27, pp. 9917–9935 (2024), doi: 10.1007/s10586-024-04458-8.
- [19] A. Kukliansky, M. Orescanin, C. Bollmann, and T. Huffmire, "Network anomaly detection using quantum neural networks on noisy quantum computers," *IEEE Transactions on Quantum Engineering*, vol. 5, pp. 1–11 (2024), doi: 10.1109/TQE.2024.3359574.
- [20] H. Qi, J. Wang, and Y. Cui, "VQCNN: Variational quantum convolutional neural networks based on quantum filters and fully connected layers," *The Computer Journal*, vol. 67, no. 10, pp. 2970–2983 (2024), doi: 10.1093/comjnl/bxae062.
- [21] C. Gong, W. Guan, H. Zhu, A. Gani, and H. Qi, "Network intrusion detection based on variational quantum convolution neural

- network,” *Journal of Supercomputing*, vol. 80, no. 9, pp. 12743–12770 (2024), doi: 10.1007/s11227-024-05919-y.
- [22] D. M. de Abreu, C. E. Rothenberg, and A. Abelem, “QML-IDS: Quantum machine learning intrusion detection system,” *arXiv preprint arXiv:2410.16308* (2024).
- [23] Z. Song, X. Zhou, J. Xu, X. Ding, and Z. Shan, “Recurrent quantum embedding neural network and its application in vulnerability detection,” *Scientific Reports*, vol. 14, Art. no. 13642 (2024), doi: 10.1038/s41598-024-63021-y.
- [24] Y. B. Gurav, M. Alagirisamy, and S. K. Selvaperumal, “Advanced quantum neural network-link net based intrusion detection framework and enhanced Blowfish cryptography for data security,” *Intelligent Decision Technologies*, vol. 19, no. 4, pp. 2401–2424 (2025), doi: 10.1177/18724981251331118.
- [25] K. C. Chen, S. Y. C. Chen, T. Y. Li, C. Y. Liu, and K. K. Leung, “Quantum machine learning for UAV swarm intrusion detection,” *arXiv preprint arXiv:2509.01812* (2025).

Received January, 2026