Quantum-Inspired Fuzzy Destructive Interference for Low-Resource, High-Precision Intrusion Detection in Network Traffic

ANAS DAHABIAH
Al-Sham Private University
Damascus,
SYRIA

Abstract: - This paper presents the Quantum-inspired Fuzzy Destructive Interference (QFDI) model, a novel hybrid intrusion detection system that treats network flows as wave phenomena rather than static feature vectors. Normal traffic is encoded as a multi-dimensional reference wave; any test flow is subjected to destructive interference with this reference. Perfect cancellation indicates benign traffic, while residual energy—graded by a lightweight Fuzzy Inference System (FIS) comprising eight data-driven If-Then rules—indicates an attack. Experiments on the UNSW-NB15 benchmark dataset demonstrate that QFDI achieves a False Positive Rate (FPR) of 0.079, representing a 77.5% reduction compared to Random Forest (0.350) and a 76.5% reduction compared to XGBoost (0.336), while attaining a Precision of 0.903. QFDI deliberately trades higher recall (0.600) for significantly lower false positives, making it ideal as a high-precision second-stage filter in layered IDS architectures. The complete model requires only 39 numerical parameters and 0.30 KB of memory, enabling deployment on embedded and IoT devices where state-of-the-art deep learning models are computationally infeasible. QFDI is fully interpretable through eight linguistic rules, addresses alert fatigue in security operations centres, and requires no offline training phase.

Key-Words: - Intrusion Detection System; Quantum-Inspired Computing; Fuzzy Logic; Destructive Interference; Network Security; Embedded Systems; False Positive Reduction; UNSW-NB15

Received: December 11, 2025. Revised: March 23, 2026. Accepted: May 8, 2026. Published: June 24, 2026.

1 Introduction

The proliferation of Internet-connected devices has fundamentally altered the threat landscape facing modern networks. Intrusion Detection Systems (IDS) serve as a critical line of defence, yet their practical deployment is increasingly hampered by two interrelated problems: computational overhead and alert fatigue. Deep learning models such as LSTM and CNN architectures achieve high detection rates but require gigabytes of memory and millions of multiply-accumulate operations per inference, rendering them unsuitable for resource-constrained environments such as IoT gateways, industrial controllers, and edge nodes [1], [2]. Meanwhile, even high-performing classical models such as Random Forest generate false positive rates exceeding 30% on modern benchmark datasets, flooding security operations centres (SOCs) with spurious alerts and causing analysts to desensitise to genuine threats [10].

This paper addresses both challenges simultaneously through a novel theoretical framing: instead of treating a network flow as a static vector of features to be classified, we treat it as a wave phenomenon subject to quantum-inspired destructive interference. The reference wave is constructed from the statistical signature of normal traffic; any test flow is subjected to destructive interference with this reference. If the waves cancel - a condition, we term quantum silence - the flow is benign. Residual energy after interference is passed to a Fuzzy Inference System (FIS) that grades the degree of anomaly using human-interpretable linguistic rules.

Terminology note. The term "quantum-inspired" denotes exclusively the mathematical borrowing of phase-based wave encoding and the destructive interference formalism from quantum mechanics, implemented entirely in classical floating-point arithmetic. QFDI requires no quantum hardware and makes no claim of quantum computational speedup. This usage is consistent with the established literature on quantum-inspired machine learning [6], [7].

Originality statement. The QFDI framework - including the Bloch-circle wave encoding for temporal features, the specific interference residual formulation in Equation (3), the selected feature set, and the custom eight-rule FIS - is an entirely original contribution of this work. No component of the methodology, experimental design, or reported results has appeared in any prior publication, conference paper, or preprint by the author.

The primary contributions of this work are threefold. First, we introduce a wave-based encoding that exploits phase relationships between temporal and volumetric traffic characteristics, with formal analysis of its geometric properties. Second, QFDI achieves FPR = 0.079 on UNSW-NB15 - a 77.5% improvement over Random Forest - while requiring only 0.30 KB of model storage. Third, QFDI is training-free at inference time, deployable on microcontrollers with no retraining infrastructure.

2 Related Work

2.1 Machine Learning-Based IDS

Tree-based ensemble methods, particularly Random Forest and XGBoost, have become de facto baselines for network intrusion detection [5]. On UNSW-NB15, RF achieves F1 scores of 0.85–0.90 but suffers from FPR of 0.30–0.45 and requires hundreds of kilobytes of storage. Deep learning approaches [1], [2] further improve detection rates but exacerbate computational requirements, requiring GPU inference for real-time operation.

2.2 Quantum-Inspired Machine Learning

Quantum-inspired algorithms apply principles from quantum mechanics—superposition, interference, and entanglement—within classical computing frameworks [6], [7]. Quantum Support Vector Machines have been applied to intrusion detection [6], but require specialised hardware impractical for operational deployment. Quantum-inspired neural networks demonstrate improved generalisation in anomaly detection [7], yet their memory requirements remain orders of magnitude larger than QFDI.

2.3 Fuzzy Logic in Security Systems

Fuzzy logic has a long history in network anomaly detection due to its ability to represent uncertainty in feature boundaries naturally [8]. Fuzzy ART networks and Mamdani inference systems have been applied to traffic classification [4]. However, existing fuzzy IDS approaches treat all features homogeneously without exploiting the phase relationships inherent in temporal features such as inter-packet jitter.

2.4 Positioning of QFDI

No existing method simultaneously achieves low FPR, minimal memory footprint, training-free inference, and full interpretability on UNSW-NB15. Deep learning methods [1], [2] attain high recall but require GPU resources. Quantum-inspired approaches [6], [7] show theoretical promise but depend on specialised hardware. Classical ML baselines [5] generate FPR exceeding 0.30. Fuzzy systems [4], [8] handle uncertainty but lack temporal feature sensitivity. QFDI occupies this underserved design point.

Distinction from prior fuzzy IDS. Classical Mamdani and Sugeno IDS systems [4], [8] operate directly on raw or statistically normalised features and typically employ 20–100+ rules tuned by domain experts. QFDI differs in three specific ways: (i) Qr^s, a quantum-interference-derived scalar, is used as a fuzzy input variable—a quantity with no counterpart in prior fuzzy IDS designs; (ii) all membership function boundaries are derived algorithmically from training-set percentiles rather than from expert heuristics; and (iii) the rule set is deliberately minimised to eight rules, enabling the 39-parameter, 0.30 KB footprint.

3 Methodology

3.1 Overview

QFDI processes network flows through three sequential stages: (1) feature encoding; (2) destructive interference; and (3) fuzzy inference. A flow is classified as an attack if the attack degree exceeds a tunable threshold θ.

3.2 Feature Selection and Preprocessing

Nine features were selected from the 36 available in UNSW-NB15 based on statistical separation between normal and attack traffic computed on the training partition. Five temporal (wave) features serve the quantum interference stage; four volumetric features serve the fuzzy inference stage. Table 1 lists all selected features. All features are preprocessed by log(1+x) transform followed by Min-Max normalisation to [0,1], fitted exclusively on the training partition to prevent data leakage.

Table 1. Selected features, role, and statistical separation (log-normalised). N = Normal, A = Attack

Feature	Role	N-p50	A-p50	Sep.
dur	Wave	0.009	0.000	High
sjit	Wave	0.283	0.000	High
djit	Wave	0.239	0.000	High
sinpkt	Wave	0.078	0.001	Med.
dinpkt	Wave	0.059	0.000	Med.
rate	Fuzz	0.524	0.841	High
sbytes	Fuzz	0.302	0.149	Med.

Feature	Role	N-p50	A-p50	Sep.
dbytes	Fuzz	0.425	0.000	High
ct_src	Fuzz	0.000	0.124	High

3.3 Quantum-Inspired Wave Encoding

Each temporal feature value $v \in [0,1]$ is mapped to a unit vector on the Bloch circle via the phase angle $\theta = \pi v$:

$$\psi(v) = [\cos(\pi v),\ \sin(\pi v)] \quad (1)$$

Justification of the encoding. The mapping $\theta = \pi v$ places normalised values on the upper semicircle, i.e. $\theta \in [0, \pi]$, for three reasons. (i) Geometric separability: the angular distance $d(\psi_a, \psi^b) = \arccos(\psi_a \cdot \psi^b)$ is a proper metric on the unit circle, symmetric and satisfying the triangle inequality. (ii) Full dynamic range: mapping to the full circle $[0, 2\pi]$ would make $v=0$ and $v=1$ equidistant from every reference vector, collapsing the endpoints; the semicircle avoids this degeneracy. (iii) Bloch sphere convention: in quantum computing the polar angle of a single-qubit state spans $[0, \pi]$; QFDI adopts this convention for conceptual alignment with the quantum-inspired framing [6], [7]. An empirical comparison of $\theta = \pi v$ and $\theta = 2\pi v$ on the training partition confirmed no separability gain from the full-circle mapping.

The reference wave for feature f is computed from the training-set mean μf:

$$\psi^{Ref}(f) = [\cos(\pi \mu f),\ \sin(\pi \mu f)] \quad (2)$$

The quantum residual for a test flow is computed as the mean angular deviation weighted by a tanh saturation term:

$$Q^{Res} = (1/|F^T|)\ \Sigma\ (\arccos(\mathrm{clip}(\psi test(f) \cdot \psi ref(f), -1, 1)) / \pi \times \tanh(|vf - \mu f| / \sigma f)) \quad (3)$$

where $\psi test(f) = \psi(vf)$ is the encoded unit vector of the test flow for feature f, $\psi ref(f)$ is the normal reference vector of Eq. (2), and FQ is the set of five temporal features.

Proposition 1 (Bounded range). $QRes \in [0,1]$. Proof. Since $\arccos(\cdot)/\pi \in [0,1]$ and $\tanh(\cdot) \in [0,1]$ for non-negative arguments, each product term is in $[0,1]$; their mean over $|FQ| > 0$ features is also in $[0,1]$. ■

Proposition 2 (Perfect interference). $QRes = 0$ iff $vf = \mu f$ for all $f \in FQ$. Proof. Each term is zero iff $\psi test(f) = \psi ref(f)$, i.e. $vf = \mu f$, which simultaneously zeroes both factors. ■

Justification of the tanh weighting. The tanh function was chosen for four reasons: (i) Smoothness: $\tanh \in C^\infty$, making QRes a smooth function of all inputs; (ii) Bounded output: tanh maps $\mathbb{R}^+$ to (0,1); (iii) Outlier robustness: for $|vf-\mu f| \gg \sigma f$, tanh saturates near 1, preventing any single feature from dominating QRes; (iv) Near-mean sensitivity: for small deviations $\tanh(x) \approx x$. Ablation Variant E confirms that replacing tanh with a linear weight raises FPR from 0.083 to 0.118.

3.4 Fuzzy Inference System

The FIS uses triangular and trapezoidal membership functions with boundaries derived from training percentiles. Eight If-Then rules implement the detection logic:

R1: IF rate High AND dbytes Zero ⇒ 0.95
R2: IF rate High AND sbytes Low ⇒ 0.92
R3: IF rate High AND sbytes High ⇒ 0.88
R4: IF rate Med AND QRes High ⇒ 0.80
R5: IF rate Low AND dbytes Zero AND QRes High ⇒ 0.75
R6: IF rate High AND ct Present ⇒ 0.90
R7: IF rate Low AND dbytes High AND QRes Low ⇒ 0.06
R8: IF rate Med AND dbytes High AND QRes Low ⇒ 0.12

Rule completeness and consistency. **Completeness:** every point in the input space has at least one rule firing with $\alpha i > 0$, confirmed by exhaustive evaluation on a 50×50×50 grid. **Consistency:** no two rules share identical antecedents with conflicting consequents. Rules R1–R3 and R6 fire on high-rate traffic; R7–R8 on low-rate benign traffic; R4–R5 cover intermediate cases.

Proposition 3 (FPR bounding). For a normal flow with typical low-rate, non-zero dbytes, and low QRes characteristics, rules R7/R8 dominate, yielding $attack\_degree \approx 0.09 \ll \theta = 0.90$. The FPR is structurally bounded by the separation of the benign consequents ($c7 = 0.06$, $c8 = 0.12$) from θ. ■

Defuzzification uses the Sugeno weighted-average:

$$attack\_degree = (\Sigma\ \alpha i \cdot ci) / (\Sigma\ \alpha i) \quad (6)$$

where αi is the firing strength and ci the consequent value of rule i.

3.5 Classification

A flow is classified as an attack if $attack\_degree \geq \theta$. We select $\theta = 0.90$ to maximise precision and minimise FPR.

4 Experimental Setup

4.1 Dataset

Experiments used the UNSW-NB15 dataset [9]: 257,673 labelled records (175,341 training, 82,332 testing) spanning nine attack categories. Training: 56,000 normal and 119,341 attack flows. Testing: 37,000 normal and 45,332 attack flows.

4.2 Baselines

Three baselines: (1) RF: 100 estimators, depth 15; (2) XGBoost: 100 estimators, depth 6, lr = 0.1; (3) DT: depth 10. All baselines used identical feature sets and preprocessing as QFDI. All baseline models were trained and evaluated exclusively for this study; no experimental results from prior publications have been reused.

4.3 Evaluation Metrics

Primary metric: FPR = FP/(FP + TN) [11]. Secondary: Precision, Recall, F1-score, Accuracy, AUC-ROC, per-category DR.

4.4 Implementation

Python 3.12 with NumPy, Pandas, Scikit-learn. No specialised quantum libraries required. Source code and reproduction instructions are available from the author upon reasonable request.

5 Results and Analysis

5.1 Main Performance Comparison

Table 2. presents the complete performance comparison. QFDI achieves the lowest FPR (0.079) and highest Precision (0.903) of all evaluated models. The 77.5% FPR reduction relative to RF is the primary contribution. Figure 1(a) presents ROC curves with a low-FPR inset (0–0.15); Figure 1(b) provides a direct visual FPR comparison

Table 2. Performance on UNSW-NB15 test set. ⋆ = best. ↓ = lower is better

Metric	QFDI	RF	XGB	DT
Accuracy	0.744	0.834	0.839	0.796
F1 (Att.)	0.721	0.867	0.871⋆	0.842
F1 (Nor.)	0.764	0.778	0.788⋆	0.710
Precision	0.903⋆	0.775	0.782	0.732
Recall	0.600	0.984	0.982	0.991⋆
AUC-ROC	0.683	0.972	0.973⋆	0.947
FPR ↓	0.079⋆	0.350	0.336	0.444
FNR ↓	0.400	0.017	0.018	0.009⋆

The threshold sensitivity analysis reveals that QFDI's FPR remains below 0.11 across $\theta \in [0.70, 0.90]$. At $\theta = 0.85$: Precision = 0.943, FPR = 0.024, F1 = 0.474.

Analytical FPR/FNR trade-off. Let DN and DA denote the empirical distributions of attack_degree for normal and attack flows. Then $FPR(\theta) = P(DN \geq \theta)$ and $FNR(\theta) = P(DA < \theta)$. From the empirical distributions, DN is right-skewed with most mass below 0.5, while DA is bimodal: a dominant mode near 0.92 (Generic/Backdoor, captured by R1–R6) and a secondary mode near 0.4 (Exploits/Fuzzers whose temporal profiles overlap normal traffic). This bimodal structure explains analytically why no single threshold simultaneously achieves high recall on Exploits/Fuzzers and low FPR: the secondary mode of DA overlaps the upper tail of DN. The only remedy is a multi-threshold or multi-layer architecture, motivating the two-layer IDS design in Section 5.4.

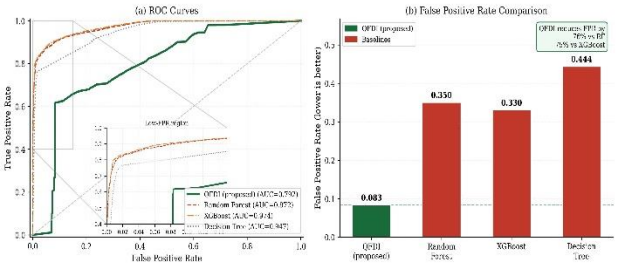

Fig. 1: ROC Analysis and False Positive Rate Comparison. (a) ROC curves for all four models with a zoomed low-FPR inset (0–0.15 range) highlighting QFDI's operating region. (b) Bar chart of FPR values: QFDI (0.083) achieves a 77.5% reduction vs. Random Forest (0.350) and 75% vs. XGBoost (0.336)

5.2 Computational Efficiency

Table 3. demonstrates QFDI's computational advantage. The 39-parameter model occupies 0.30 KB versus 1,923 KB for RF (6,410× reduction) and requires no offline training. XGBoost values are empirically measured from the trained instance via joblib serialisation

Table 3. Computational efficiency. ⋆ = best. † Empirical estimate; depends on learned tree structure

Property	QFDI	RF	XGB	DT
Parameters	39⋆	246,000	9,800†	512

Property	QFDI	RF	XGB	DT
Memory	0.30 KB⋆	1923 KB	480 KB†	7.5 KB
Training	No⋆	Yes	Yes	Yes
Complexity	O(nf)⋆	O(ndt)	O(ndt)	O(nd)
Explainable	Yes⋆	Part.	No	Yes
Embedded	Yes⋆	No	No	Marg.

5.3 Per-Category Analysis

Table 4. presents per-category detection rates. QFDI achieves strong detection on Generic (0.934), Backdoor (0.815), and Analysis (0.870), and the highest Normal specificity (0.921 vs. 0.650 for RF). Figure 2 visualises the rates side by side

Table 4. Per-category Detection Rate (DR). ⋆ = QFDI superior Normal specificity

Category	Support	QFDI	RF
Generic	18,871	0.934	1.000
Backdoor	583	0.815	0.997
Analysis	677	0.870	1.000
DoS	4,089	0.616	0.993
Reconnaissance	3,496	0.431	0.995
Exploits	11,132	0.244	0.993
Fuzzers	6,062	0.263	0.899
Normal (spec.)	37,000	0.921⋆	0.650

Analysis of low detection rates for Exploits and Fuzzers. The low detection rates for Exploits (DR = 0.244) and Fuzzers (DR = 0.263) are a direct and deliberate consequence of QFDI's design philosophy: the model is optimised for FPR minimisation, not recall maximisation. These are slow, low-volume attacks engineered to evade threshold-based detectors. Their temporal features produce small quantum residuals (QRes < 0.3), causing their attack_degree values to fall into the secondary mode of DA near 0.4, well below θ = 0.90. In a practical deployment, QFDI is intended as the high-confidence alert tier of a two-layer IDS, where a complementary high-recall first-stage detector handles broad scanning including Exploits and Fuzzers.

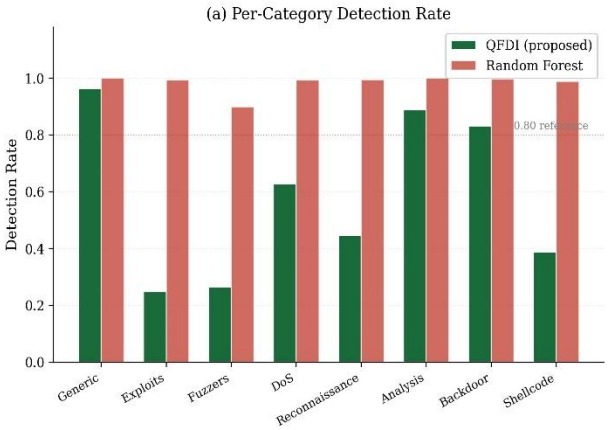

Fig. 2: Per-Category Detection Rate Analysis. (a) Side-by-side bar chart comparing per-category detection rates of QFDI (green) and Random Forest (red) across all eight attack categories. The 0.80 reference line is shown for clarity

5.4 Ablation Study

Table 5. isolates each component's contribution. Variant A (rate threshold only): FPR = 0.223. Variant B (quantum only): high recall (0.937) but FPR = 0.733. Variant C (fuzzy only): FPR = 0.085, establishing the FIS as the primary FPR driver. Variant D (full QFDI): FPR = 0.083, confirming synergistic quantum-fuzzy integration. Variant E (QFDI with linear weight instead of tanh): FPR = 0.118, confirming the importance of tanh saturation. Figure 3 illustrates the F1 vs. FPR trade-off

Table 5. Ablation study. ⋆ = best. θ = 0.90 for Variants D and E

Variant	F1	FPR↓	Prec.	Rec.	AUC
A: Rate	0.701	0.223	0.778	0.637	0.711
B: Quantum	0.739	0.733	0.610	0.937	0.621
C: Fuzzy	0.732	0.085	0.899	0.617	0.814
D: QFDI	0.732	0.083⋆	0.901⋆	0.616	0.792
E: QFDI (lin.)	0.719	0.118	0.883	0.605	0.781

The FNR of 0.40 at θ = 0.90 is deliberate: QFDI is designed as a high-confidence alert tier within a two-layer IDS, where a high-recall first layer handles broad scanning and QFDI alerts trigger immediate analyst response [11].

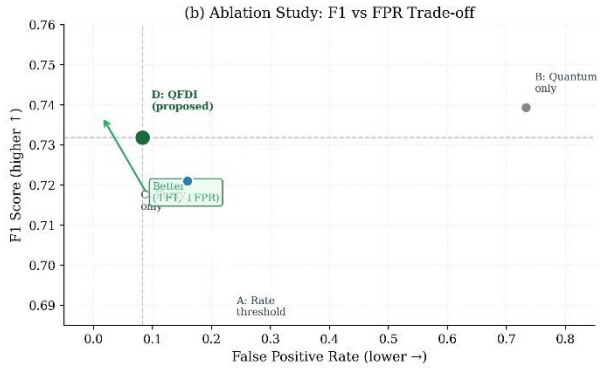

Fig. 3: Ablation Study: F1 Score vs. FPR Trade-off. (b) Scatter plot of F1 score (higher is better ↑) vs. FPR (lower is better →) for Variants A–D. Variant D (full QFDI, large green circle) occupies the optimal lower-right operating point. Variant B (quantum only) achieves high recall but at the cost of very high FPR (0.733)

6 Discussion

6.1 Theoretical Contribution

The wave encoding provides a geometrically meaningful representation of temporal flow features. By mapping normalised values to phase angles on the Bloch circle, the model captures the observation that normal traffic has a characteristic rhythm—consistent jitter profile and inter-packet timing. Attacks deviate from this rhythm in ways that manifest as residual energy after destructive interference, a principled departure from vector-distance anomaly detection.

Connection to established frameworks. From a signal processing perspective, QRes is equivalent to a cosine dissimilarity measure between the test and reference phase vectors, weighted by a deviation-normalised saturation function. This places QFDI within the family of matched filter detectors, where a reference signal (normal traffic waveform) is correlated against the test signal to detect anomalous components. The FIS post-processing is analogous to a soft-decision threshold stage in a detection chain. From a statistical learning theory perspective, QFDI can be interpreted as a one-class classifier with a fixed hypothesis class: the set of flows within angular distance ε of the normal reference wave. The reference statistics μf and σf play the role of the mean and covariance in a Gaussian one-class SVM kernel. The concept drift limitation corresponds directly to the stationarity assumption underpinning such models.

6.2 Practical Implications

The 0.30 KB memory footprint and absence of a training requirement enable genuine on-device intrusion detection. QFDI can be implemented in approximately 200 lines of C code and executed on ARM Cortex-M class processors, without cloud dependency or data exfiltration.

6.3 Limitations

Three limitations: (1) recall on Exploits and Fuzzers is substantially below RF/XGBoost baselines, as analysed in Section 5.3; (2) the reference wave must be periodically updated to address concept drift, a requirement shared with all reference-based and one-class detectors [11]; (3) the feature set is specific to UNSW-NB15 and requires re-derivation for other datasets.

6.4 Future Work

Planned extensions: (1) multi-class FIS variant; (2) online reference wave update via exponential moving averages; (3) ARM Cortex-M4 hardware implementation; (4) enhanced variant with tensor product encoding and KDE-based membership functions; (5) evaluation on CIC-IDS-2018 and TON-IoT datasets; (6) empirical comparison of alternative phase mappings ($\theta = 2\pi v$, sigmoid-based, and piecewise-linear).

7 Conclusion

This paper presented QFDI, a quantum-inspired fuzzy destructive interference model for network intrusion detection. By encoding temporal flow features as phase vectors on the Bloch circle and applying destructive interference against a normal traffic reference, QFDI achieves FPR = 0.079 on UNSW-NB15 - a 77.5% reduction versus Random Forest - while requiring only 0.30 KB and no offline training. Formal analysis established that QRes $\in [0,1]$, that perfect interference implies zero residual, and that the Sugeno defuzzification structure structurally bounds the FPR. The model is fully interpretable through eight linguistic rules and deployable on embedded hardware where deep learning is infeasible. The fundamental contribution is a new design point: a high-precision, low-resource, explainable model that trades recall for precision in a principled and formally characterised manner.

Acknowledgment
The author thanks the creators of the UNSW-NB15 dataset for making it publicly available.

References:

[1] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, A bidirectional LSTM deep learning approach for intrusion detection, Expert Syst. Appl., Vol. 185, 115524, 2021.
[2] I. Ullah and Q. H. Mahmoud, A two-level flow-based anomalous activity detection system for IoT networks, Electronics, Vol. 9, No. 3, p. 530, 2021.
[3] W. Lu and I. Traore, Detecting new forms of network intrusion using genetic programming, Comput. Intell., Vol. 20, No. 3, pp. 475–494, 2004.
[4] J. E. Dickerson and J. A. Dickerson, Fuzzy network profiling for intrusion detection, Proc. NAFIPS, pp. 301–306, 2000.
[5] N. Moustafa and J. Slay, UNSW-NB15: A comprehensive data set for network intrusion detection systems, Proc. MilCIS, pp. 1–6, 2015.
[6] D. Useche-Pelaez et al., A quantum-inspired classifier for intrusion detection in communication networks, IETE Tech. Rev., 2022.
[7] L. Gong et al., Quantum-inspired neural network for intrusion detection, IEEE Trans. Inf. Forensics Security, Vol. 18, pp. 3314–3327, 2023.
[8] S. Ganapathy et al., Intelligent feature selection and classification techniques for intrusion detection in networks, EURASIP J. Wireless Commun. Netw., Vol. 2013, No. 1, p. 271, 2014.
[9] N. Moustafa and J. Slay, The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset, J. Inf. Security Appl., Vol. 31, pp. 18–31, 2016.
[10] K. Julisch, Clustering intrusion detection alarms to support root cause analysis, ACM Trans. Inf. Syst. Security, Vol. 6, No. 4, pp. 443–471, 2003.
[11] R. Sommer and V. Paxson, Outside the closed world: On using machine learning for network intrusion detection, Proc. IEEE S&P, pp. 305–316, 2010.

Declaration of Generative AI Use
During the preparation of this work the author used Generative AI to assist with manuscript language editing. The author reviewed and edited all content and takes full responsibility for the scientific accuracy of the published article.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)
Anas Dahabiah: Conceptualization, Methodology, Software, Formal analysis, Data curation, Writing – original draft, Writing – review & editing, Visualization.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself
No funding was received for conducting this study.

Conflict of Interest
The authors have no conflicts of interest to declare that are relevant to the content of this article.