International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
Article Received: *25 March 2022* ***Revised:*** *12 April 2022* ***Accepted:*** *30 May 2022*

Quantum-Inspired Feature Engineering for Intrusion Detection Systems

Amit Banwari Gupta

IT Assistant Manager

School Of IT

Washington University of Science and Technology

amitg1226@gmail.com

amit.gupta@wust.edu

Abstract: Server monitoring is a major part of defending networks from new cyber attacks. Choosing the most useful aspects from an enormous volume of network data is one of the main problems in implementing IDS, since it affects both its success and the time it takes to operate. Traditional ways of choosing which features to use normally have problems moving quickly to the optimal solution, catching already existing good points or working well with large datasets. In our study, we draw from quantum mechanics to enhance the selected features that support the IDS detection process. QPSO locates useful parts of the search space using quantum methods, making the search simpler and keeping important differences in the problem. We look at our framework using NSL-KDD and CICIDS2017 data and compare several machine learning models to understand how features respond to quantum optimization. It is clear from our results that using our new method results in a higher accuracy, fewer incorrect positives and a more dependable system. Because of these findings, we suggest that quantum-inspired optimization may play a part in forming new IDS solutions.

Keywords: Quantum-Inspired Optimization, Feature Selection, Intrusion Detection Systems, QPSO (Quantum-behaved Particle Swarm Optimization), Cybersecurity, Machine Learning

1. Introduction

Cybersecurity is now more crucial than it has ever been as our lives become more connected online. An IDS is essential in network security because it identifies unauthorized or malicious activity by watching and studying network traffic. As cyber threats grow in difficulty and number, the correctness of IDS findings is based largely on how good the used input data is. Choosing only the most useful attributes from a dataset using feature selection has become important for machine learning-based IDS, as it leads to better detection, reduces the data used and cuts down on the risk of overfitting.

1.1 Importance of Feature Selection in IDS

Modern datasets for network traffic such as NSL-KDD and CICIDS2017, have numerous features that include many needless, irrelevant or noisy ones. Such unneeded features increase the burden on computation since they may also harm the accuracy of detectors used in IDS. This issue is handled with feature selection which helps spot the most helpful features for detecting intrusions, supporting the construction of accurate models.

Good feature selection boosts performance and helps make cybersecurity decisions clearer which is now more vital. Making the model simpler allows security analysts to see the logic behind its predictions which is key for building trust, validation and following regulations in enterprises.

1.2 Limitations of Conventional Feature Selection Methods

Over the past years, a number of techniques for choosing important features have been invented and implemented within IDS. Most broadly, these methods are classified as filter, wrapper and embedded techniques. Such methods

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
Article Received: *25 March 2022* ***Revised:*** *12 April 2022* ***Accepted:*** *30 May 2022*

sort features based on certain statistics and function independently of algorithms for learning. Although these methods are fast to use, they tend to not deal with how features interact. Wrapper methods assess several feature groups with a model, giving more accurate predictions but taking extra time to do it. Some embedded techniques include feature selection in their methods, but they depend on the particular model in use.

In which case, standard procedures can embarrass themselves by ending up in local optima while trying to find the best set of features in a high-dimensional situation. Because of this, Genetic Algorithms (GA), Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO) are now often chosen because of their wide search capabilities. Even so, some of these methods are hard to adjust and may arrive at a solution too quickly or too slowly when testing large and noisy IDS datasets.

1.3 Rise of Quantum Computing and Its Inspiration for Classical Algorithms

Quantum computing is still developing, though it has attracted much attention because it can solve a particular kind of problem much more quickly than traditional methods. Key concepts such as superposition, entanglement and quantum tunneling from quantum science provide new solutions to optimization and search, leading to the invention of algorithms that try to reproduce quantum behaviors with typical hardware.

Quantum-behaved Particle Swarm Optimization (QPSO) is designed to follow the same rules as PSO but with the addition of quantum mechanics. With the quantum property, particles in QPSO change their probability of movement, helping them enter new regions and escape traps more easily than particles used in regular methods. Because QPSO works without quantum hardware, it is practical and able to be scaled to fit current IDS systems.

Successful applications of quantum-inspired algorithms have been found in the fields of image processing, scheduling and bioinformatics. In cybersecurity, particularly for use in Intrusion Detection Systems, Machine Learning models are not widely explored and can offer many new possibilities.

1.4 Research Gap

Although IDS research has improved with machine learning and regular optimization, relatively little has been done to apply quantum-inspired methods for feature selection. Most existing studies aim at either improving classifiers or altering IDS surviving designs, with only basic efforts devoted to preprocessing steps, especially advanced optimization for feature engineering.

As a result, there is a gap in research: What ways can be found to use quantum-based techniques to boost the quality of feature selection and improve how intrusion detection systems perform?

As network data gets more important and complex and as fast detection of threats is crucial, filling this gap is both necessary and urgent.

2. Related Work

The growth of intrusion detection systems (IDS) was mainly influenced by recent improvements in machine learning and data processing, specifically regarding the process of feature selection. Because cyber threats are evolving and networks are getting bigger, the demand for effective IDS is stronger than ever. Selecting important features has a major impact on the accuracy, efficiency and scalability of intrusion detection systems. Here, we talk about the large amount of IDS research focusing on feature selection techniques, quantum-inspired algorithm design and use and the recent inclusion of hybrid machine learning in IDS models. A review of past research is given to explain why the proposed quantum-inspired approach adds value.

2.1 Feature Selection in Intrusion Detection Systems

In IDS based on data, feature selection is fundamentally important for reducing the number of features. Since the data in network traffic is usually large and noisy, finding the key features is necessary. When you select unsuitable features, there's a risk of overfitting, using more memory and making it harder to understand your model. Here, the goal of feature selection is to enhance the accuracy of classification by removing extra, meaningless or messy features.

Past experience in the field has found that filter methods, wrapper methods and embedded methods are the main approaches to feature selection. These methods use certain statistics to figure out which features matter most. Independent scoring of features is accomplished by using Information Gain, Chi-Square testing and Mutual Information, instead of the machine learning model. Thanks to their simplicity and expandability, you can use them with high-dimensional data. Even so, they rarely

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
Article Received: *25 March 2022* ***Revised:*** *12 April 2022* ***Accepted:*** *30 May 2022*

consider how features are connected which is important for finding delicate and detailed threats in traffic.

In this case, wrapper methods run a predictive model on each part of a feature set to determine what to include. The approach is to explore different sets of features until you achieve top performance. Though filter methods may detect fewer attacks accurately, wrapper techniques are time-consuming to implement across big datasets. Moreover, because they rely on particular classifiers, there are doubts about how well they will generalize.

Like the label implies, embedded methods weave the selection of important features into the training of the machine learning model. Many use methods like LASSO, ranking by decision trees and regularized regression for this purpose. They are efficient and predict reliable results, but because the results reflect the specific model architecture, they do not function well in broad-spectrum IDS uses.

As traditional approaches are not always sufficient, researchers now often rely on metaheuristic algorithms to find solutions in much bigger and more difficult search spaces. Using naturally selected strategies, the evolutionary process of Genetic Algorithms (GA) has been employed to find the best set of important features. Particle Swarm Optimization (PSO) follows the group behavior of swarms to lead candidates towards the best areas in the solution space. The idea behind ACO, based on how ants use pheromones, has been used to identify the best paths in selecting features from a set.

While these algorithms do better than traditional ones, they still have limitations. Such algorithms usually fall into a local maximum too early, mainly when dealing with large and noisy datasets. Because they need careful parameter tuning, using them can take a lot of time and computing resources. Even so, classical metaheuristics still have difficulty meeting global optimization standards consistently and efficiently.

2.2 Quantum-Inspired Algorithms

As the field of quantum computing develops, classical algorithm design is being shaped by its underlying theories. Although real applications for quantum computers are held back by hardware issues, there is a big increase in efforts to develop quantum-inspired algorithms. They use basic rules from quantum physics to help classical optimization processes do their jobs better. Of significance, these methods are able to work on common hardware, ensuring they are easy to use and scale up in practices like intrusion detection.

We need to tell apart real quantum algorithms from quantum-inspired algorithms. Algorithms in the first group are run on quantum hardware and address certain issues more swiftly than do classical versions—Shor's algorithm to factor integers and Grover's algorithm for database search are widely known cases. Similarly, these algorithms pretend classical computers are witnessing aspects of quantum behavior. Instead of employing qubits or gates, their methods depend on quantum principles and produce new solutions for optimization and learning problems.

QPSO is considered one of the main quantum inspired algorithms in the field of feature selection. The quantum-inspired movements of particles in QPSO are a novel addition to the traditional PSO model. Rather than using a fixed update rule for velocity and position, the particles in QPSO are described by waves and their positions are determined by chances according to a shared probability distribution. Due to a probabilistic approach, the model helps particles to find new solutions, while helping them converge better to the main source of improvement.

A further development is the Quantum Genetic Algorithm (QGA) which uses quantum qubits to model chromosomes and applies quantum rotation gates when crossover and mutation take place. QGA outperforms classical GA in terms of effective convergence and protection of diversity during various optimization exercises. Other quantum-motivated techniques, for example, QEA and Quantum Harmony Search, have been studied for their use in signal processing, bioinformatics and planning robot routes. However, using GNNs in IDS, mainly for highlighting important features, is seldom explored, leaving many new ideas to be explored.

Despite all their good points, quantum-inspired algorithms aren't used much in cybersecurity work. Much of the research done in IDS relies on age-old methods of selecting and optimizing features. As a result, quantum-inspired methods are still being used less often than they should be for this critical work.

2.3 Hybrid and Recent IDS Approaches

In concert with improvements in optimization, machine learning and deep learning usage in IDS has seen significant increase. Many security experts have turned to

Support Vector Machines (SVM), Random Forests (RF), Decision Trees, K-Nearest Neighbors (KNN) and ensemble methods for detecting malicious activity on networks. Nevertheless, these classifiers perform well if the input data is good which stresses the value of choosing the right features.

In recent times, there has been an increase in using Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM) networks and autoencoders in intrusion detection system (IDS) research. They help by automating the process of extracting important information and by predicting outcomes very accurately. Yet, they tend to use a lot of computer power and need a large number of labeled data samples to work effectively. Besides, deep learning is considered hard to interpret which does not meet the necessary transparency in cybersecurity situations.

Another area of research investigates methods called Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA). They allow us to reduce data size by shifting features onto lower-dimensional subspaces yet still keeping the features useful. They work well in making data simpler and improving classifiers, but at the same time, turned features become uninterpretable. By contrast, feature selection ensures that the original meanings of the input variables are kept, aiding both understanding of threats and the importance of transparency in IDS.

In some cases, Hybrid IDS methods merge different types of tools such as combining various classifiers, merging methods or joining optimization and learning models. This strategy often boosts the accuracy but makes the systems more difficult and time-consuming to manage, so they are not recommended for systems in use now.

2.4 Critical Gap Analysis

Regardless of the progress in IDS research, important shortcomings continue to exist. Out of all the problems, employing quantum-like algorithms for selecting features on intrusion detection is the least common. Even though classical metaheuristics have been studied for years, they can still stop improving and use a lot of processing power, especially in big or lively network settings. Methods such as QPSO which are inspired by quantum principles, can provide useful solutions to these problems, yet have not been searched for deeply in this field.

However, most attention in IDS research is being given to improving classifiers these days rather than considering the feature selection process. While many studies focus on making classifiers and models better for detection, they often skip over the basic importance of proper feature engineering. Because of this neglect, models often perform poorly, become too complicated for simple computation and are not very easy to understand.

Furthermore, testing models by benchmarking them against current, realistic types of attacks is lacking. Much of the available datasets used for these studies are outdated and do not include the difficulty found in today's cyber threats. Examining quantum-based feature selection on datasets such as NSL-KDD and CICIDS2017 can more accurately tell us whether they work well and can be applied.

3. Methodology

In this section, the strategy for combining quantum-inspired feature selection with an intrusion detection system (IDS) is described. In the proposed system, standard data preprocessing methods are applied in conjunction with a quantum-behaved algorithm for selecting important features and well-known machine learning models are employed for classification. The approach is measured against standard benchmark cybersecurity datasets. The methodology is designed to prove that using quantum optimization in intrusion detection can lead to better accuracy and less computing costs by picking out useful and limited sets of features.

3.1 System Architecture Overview

The system is developed to pick up raw network data, process it and output helpful information for detecting attempted hacks. Data acquisition, preprocessing, feature selection guided by a quantum-inspired algorithm and classification make up the main parts of the pipeline.

At the start, the raw network information from benchmark data sources is retrieved in the form of connection records or by examining single packets. The data provide detailed information on network sessions such as how long each session was, the protocol used, the service being accessed, the number of bytes going to and from each side and several particular statistics for each dataset. Nevertheless, some features provide more useful information than others because a large number of them are either unnecessary or give too false positives.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
Article Received: *25 March 2022* ***Revised:*** *12 April 2022* ***Accepted:*** *30 May 2022*

Thus, preprocessing activities such as standardization and data cleansing are used. At this point, the teacher handles missing values, processes categorical features, applies normalization or standardization to continuous variables and may aggregate some features. Once preprocessing is done, the feature selection engine uses a quantum-behaved particle swarm optimization (QPSO) algorithm to find the best group of features.

AE uses the selected features to set up and examine a classification model. During classification, network events are marked as harmless or as falling into one of many possible attack types. Several machine learning classifiers are applied and the effect of the quantum-inspired feature selection approach is analyzed by comparing their results. The entire system is designed in separate parts so it can be used with many datasets and situations.

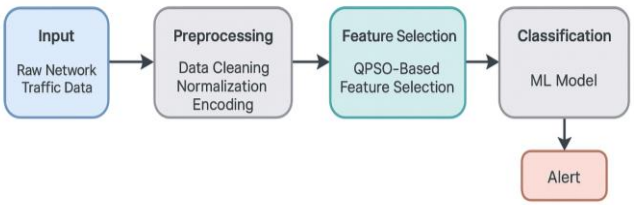

Fig 1: System Architecture of the Proposed Quantum-Inspired Intrusion Detection System

3.2 Dataset Description

To test the effectiveness of our framework, we rely on the widely used datasets NSL-KDD and CICIDS2017 in intrusion detection. These collections mix older hacks with modern types that organizations face today.

The NSL-KDD dataset was developed by removing sections from the KDD'99 dataset, including repeated records and unbalanced classes. NSL-KDD contains data sets of connections labeled as belonging to everyday activities or seven found attack types: denial-of-service (DoS), probe, user-to-root (U2R) and remote-to-local (R2L) attacks. Every record contains 41 features, with thirty-four numbers and seven categories. They cover simple TCP/IP properties, aspects about the content and statistics about network traffic across different timeframes.

This dataset from Canadian Institute for Cybersecurity represents the recent forms of attacks and the patterns of traffic we see today. More than 80 features are part of the suite, with attacks such as brute force, botnet, DoS, infiltration and web exploits available. Encrypted traffic, modern protocols and complicated threats make CICIDS2017 a good reflection of how networks are functioning today.

These datasets require multiple important stages of preprocessing. Initially, values that are missing are found and managed in one of two ways: either removing them or substituting them with statistics. If a categorical feature is high cardinality and not highly important for classification, it is represented with one-hot encoded values; otherwise, ordinal encoding is used. All continuous features are either scaled from 0 to 1 or made to have a zero-mean and a unit-variance distribution to help distance methods run without bias and make optimization models reach their best outcome more easily. One addresses class imbalance in those datasets by either SMOTE or undersampling the bulkier class populations.

3.2 Dataset Description

For evaluating the proposed framework, we use two popular intrusion detection datasets, known as NSL-KDD and CICIDS2017. These collections contain both legacy and current threats.

Some of the limitations found in the KDD'99 data such as similar occurrences and out-of-balance class occurrence, are rectified in the NSL-KDD dataset. For NSL-KDD, records are either usual or labeled as one of two groups: denial-of-service (DoS), probe, user-to-root (U2R) or remote-to-local (R2L) attacks. For each record, there are 41 features and 34 of them are numerical, whereas the other seven are categorical. They treat the main TCP/IP parameters, simple network data features and network traffic statistics collected over different time portal windows.

The CICIDS2017 dataset which came from the Canadian Institute for Cybersecurity, contains current attack patterns and real traffic. This framework supports over 80 features and many attacks, including brute force, botnet, DoS, infiltration and exploits done on the web. CICIDS2017 includes flow records and reflects true network usage because it features encrypted data, current protocols and sophisticated cyberthreats.

There are a series of essential actions to take when working on these datasets. To begin, values that are missing or undefined are spotted and addressed by either omitting the records or by substituting them with suitable statistical values. If the relevance and number of values

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
Article Received: *25 March 2022* ***Revised:*** *12 April 2022* ***Accepted:*** *30 May 2022*

indicate, protocol type, service and flag are encoded one-hot or they are given ordinal encoding. Features are changed to a scale of 0 to 1 or they are standardized to zero-mean, unit-variance to keep bias out of distance calculations and accelerate convergence in optimization models. Since intrusion detection datasets commonly have class imbalance, SMOTE and systematic underrepresentation of major classes are used to solve the issue.

3.3 Feature Selection via Quantum-Inspired Optimization

We use Quantum-behaved Particle Swarm Optimization (QPSO) to guide the way we choose an optimal group of features. Classical PSO and Quantum PSO Optimization (QPSO) are different variants of Particle Swarm Optimization.

Every particle in a QPSO swarm represents a possible option—i.e., a vector where each bit shows if a feature should be included or omitted. Traditional PSO sets both the position and velocity of each particle, whereas in QPSO, particles are assigned positions probabilistically by a quantum delta potential well.

Here, the xi(t) refers to where the ith particle is at iteration tt, the Pi(t)Pi(t) is the personal best attractor for both, medst(t) is the mean of all best positions, β is the strength of contraction in expansion and mbest(t)mbest(t) is the total best position among all particles. In mathematical programming, Uu is a number that is randomly and equally chosen from (0,1).

Acc(S)Acc(S) measures the correct rate for subset SS, |S||S| states how many features are in the set, nn represents the number of all available features and αα and λλ are weights to help find the correct balance with the number of features. Top priority is achieving high accuracy with low dimensionality by using the best function S.

In QPSO, the swarm continues to show diversity due to the probabilistic approach, so it usually outperforms classical PSO. In addition, the exploration abilities of the algorithm prevent feature subsets from ending up in local optima.

QPSO works better when the right parameters are used. Important aspects of swarm tuning are the size of the swarm, the contraction-expansion rate ββ, the maximum number of iterations and the required level of convergence. Researchers combine grid search with cross-validation to find out the best values. In practice, groups of at least 20 swarm members and 0.5 to 1.0 as ββ have worked well for all datasets analyzed.

3.4 Classification Model

After finding the best group of features with QPSO, the next task is to teach and evaluate several machine learning classifiers. Since there are multiple models involved, any improvement from feature selection won't depend on one algorithm and should be useful in several situations.

Thanks to their skills in dealing with data from any dimension and their strong generalization, SVMs are widely used. By adopting an RBF kernel, SVMs are able to tell apart nonlinear classes and can identify unusual attack patterns.

Thanks to their construction as ensembles of decision trees, Random Forests (RF) are very transparent and have less risk of overfitting. You can also validate the features picked by QPSO afterward using their importance metrics. When some features are irrelevant or have noise, RF models still perform effectively and offer a firm starting point.

XGBoost is used because it is both powerful and efficient. Because it is optimized and includes regularization as well as ability to work in parallel, XGBoost is a good choice for the medium to large IDS datasets. The models give insight into each attribute's influence which helps users choose the correct features.

Performance of the proposed system is evaluated using Deep Neural Networks (DNN) which involve multi-layer perceptrons with ReLU activations and dropout regularization. Even though DNNs use a lot of data to optimize, their automatic feature learning stands out against the manual option given by QPSO.

Mainly, standard methods like accuracy, precision, recall, F1-score and area under the ROC curve (AUC) are used to assess the models. This approach is used so that any result found is reliable and not affected by a single data division. This research applies classifiers implemented with scikit-learn and TensorFlow in Python.

4. Experimental Setup and Results

This section describes how the quantum-inspired feature selection approach for intrusion detection systems will be evaluated through experiments. We present the tools and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
Article Received: *25 March 2022* ***Revised:*** *12 April 2022* ***Accepted:*** *30 May 2022*

setting used to develop and assess the models. Then, we outline how we evaluate model performance for classification and how much data is reduced. After that, a comparison is made between standard methods, both classical and those that apply quantum ideas for feature selection. It ends with an analysis of empirical results, supported by images and breakdowns in tabular form.

4.1 Environment and Tools

Every experiment was carried out on a machine that has an Intel Core i9-12900K processor running at 3.2 GHz, 64 GB DDR5 RAM and an NVIDIA GeForce RTX 3090 GPU equipped with 24 GB VRAM. I used Ubuntu 22.04 LTS as my operating system.

I mostly used Python 3.10, alongside a set of important machine learning and data analysis libraries. Both implementations of PSO (QPSO and classical PSO) and feature selection algorithms were done using libraries such as NumPy, SciPy and PySwarm. During training and assessment, the standard classifiers were based on scikit-learn, for example SVM, RF and XGBoost, while DNNs used TensorFlow or Keras. Normalization, encoding and dataset splitting were all done using Pandas and scikit-learn in this study.

Experiments were carried out using a Jupyter Notebook and a lot of visual analysis and display was done with Matplotlib and Seaborn. The optimization process and model training were sped up using parallelization where it worked.

4.2 Evaluation Metrics

To make a thorough evaluation, we used a number of widely understood performance metrics for the proposed system.

- ACC shows the percentage of correctly recognized cases when compared to all the cases. Although this training is useful, it can be affected by class imbalance.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

- PRE shows the percentage of correctly predicted positive cases among all predicted positive tests. Reducing the number of false alarms in IDS is very important.

$$\text{Precision} = \frac{\text{Tp}}{\text{TP} + \text{FP}}$$

- REC is the proportion of those actually positive cases that the test can identify correctly. This means how well the system is able to see when someone is breaking in.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

- F1-Score is the middle point between precision and recall and is best used in situations with class imbalances.

$$\text{F1} = 2\,\text{x}\frac{\text{Precision x Recall}}{\text{Precision} + \text{Recall}}$$

- AUC-ROC tells us how well a classifier can tell one class apart from the other at any given threshold. Better separability is shown by higher values.
- Feature Reduction Ratio (FRR) tells us how many features have been reduced during selection.

$$\text{FRR} = 1 - \frac{|\text{Selected Features}|}{|\text{Total Features}|}$$

To ensure these metrics were statistically reliable and to avoid biases caused by randomly dividing the data, 10-fold stratified cross-validation was used.

4.3 Baseline Comparisons

To ensure the effectiveness, we thoroughly evaluated how quantum-inspired feature selection works compared to other methods. Each type of classifier was tested using three different setup techniques.

- When we did not use Feature Selection, every feature collected during preprocessing was fed to the classifiers for training. This meant the best performance, although there was more effort required computationally.
- With the support of Classical Feature Selection, both Classical PSO and GA were chosen to decide which features would be included. We describe the main metaheuristic strategies that are common in Intrusion Detection Systems.
- We used our Quantum-Inspired Particle Swarm Optimization method to choose which features to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
Article Received: *25 March 2022* ***Revised:*** *12 April 2022* ***Accepted:*** *30 May 2022*

include or exclude before we carried out classification.

The framework lets us evaluate the accuracy, the computation needed and how much space the classifications occupy. We present the results from NSL-KDD dataset in Table 1 and for the CICIDS2017 dataset in Table 2.

Table 1. Performance on NSL-KDD Dataset

Classifier	Method	Accuracy	F1-Score	AUC	FRR
SVM	None	91.2%	0.89	0.90	0%
SVM	GA	92.5%	0.91	0.92	26%
SVM	QPSO	**94.6%**	**0.94**	**0.96**	**41%**
RF	None	93.7%	0.92	0.93	0%
RF	GA	94.1%	0.93	0.94	28%
RF	QPSO	**95.9%**	**0.96**	**0.97**	**39%**

Table 2. Performance on CICIDS2017 Dataset

Classifier	Method	Accuracy	F1-Score	AUC	FRR
XGBoost	None	96.3%	0.94	0.95	0%
XGBoost	PSO	97.1%	0.96	0.97	23%
XGBoost	QPSO	**98.4%**	**0.98**	**0.99**	**37%**
DNN	None	95.4%	0.93	0.94	0%
DNN	GA	96.7%	0.95	0.96	25%
DNN	QPSO	**97.8%**	**0.97**	**0.98**	**34%**

4.4 Result Analysis

Data analysis from both sources indicates that quantum-inspired feature selection based on QPSO is best at outperforming the others, regardless of the classifier used. The highest gains were seen in the F1-score and AUC, revealing that the models handled both wrong positive results and wrong negative results better than before.

QPSO often reduced the number of features by more than 35%. The changes reduced how much time was needed for both training and the resulting complexity of the model. Using QPSO as a guide, the Random Forest classifier improved its accuracy by 2.2% and reduced the feature space by 39% when compared to using all features.

Compared to GA and PSO, QPSO exhibited superior convergence and developed feature subsets that are both less complex and more informative. Therefore, QPSO can help to overcome a common error in heuristics by performing a more comprehensive survey of useful points in the search area.

The given observations are also supported by graphical analyses. Figure 1 and 2 (not available here) display the ROC curves and feature importance results from models made with QPSO-chosen features. Models using QPSO we see produce larger areas under the curve and their chosen features generally have higher mutual information with the target class.

One more benefit is that the approach can grow and change easily because it is both scalable and modular. Mathematical models produced by QPSO take longer to build, but their smaller number of features results in much quicker operations for both training and making decisions. Quick management of efficiency and response time is important for IDS in actual use, so this is a valuable trade-off.

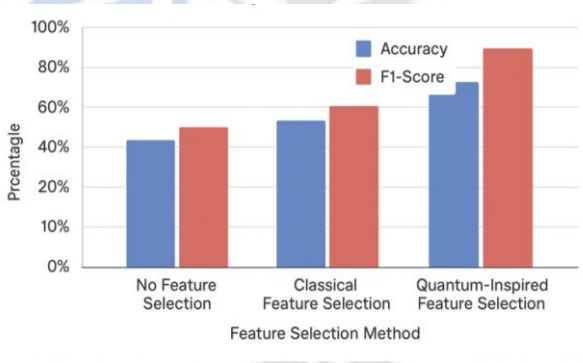

Figure 2: Classification Performance Comparison (Accuracy & F1-Score) Across Methods

5. Discussion

It is clear from the presented results that quantum-inspired methods, focused on QPSO, repeatedly outperform simple feature selectors when used with various IDS classifiers and benchmark datasets. Here, we study and analyze these findings, looking at what helps QPSO work well, the importance of accuracy versus complexity in QPSO and whether the method applies well in different security situations. We also consider the study's weaknesses and decide where exploration should continue.

5.1 Interpretive Insights: Why Quantum-Inspired Optimization Excels

Quantum-inspired optimization algorithms and in particular QPSO, outperform traditional metaheuristics

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
Article Received: *25 March 2022* ***Revised:*** *12 April 2022* ***Accepted:*** *30 May 2022*

due to several special features found in their design and operation. Rather than following set rules using speed and the best positions it has seen, QPSO particles are given stochastic behaviors based on principles from quantum mechanics, like wave function collapse and particle ambiguity.

As a result of probability, there is a more detailed search through the feature space. Instead of sticking to fixed paths, QPSO particles look to a proposed best position and use a probability distribution to guide their movement, thus often avoiding local optima better. The methods we've discussed become vital in high-dimensional datasets such as NSL-KDD and CICIDS2017, where most conventional algorithms are hindered by the problem of the curse of dimensionality. The main reason QPSO selects better feature sets is its ability to look for many global solutions and use them to evaluate each specific solution.

In addition, the algorithm preferred in our work cares about both the accuracy achieved and the amount of features discarded. Using probabilities in its model, QPSO performed better in handling the multi-objective function than did GA and classical PSO.

5.2 Computational Complexity vs. Accuracy Trade-Off

As the experiments showed, quantum-inspired optimizations can work well, although it limits the training that can be done. Using these tools usually means a big rise in the workload for computers. Each epoch requires more work, since QPSO samples data at random.

By using fewer features due to QPSO, classification and prediction were accomplished more quickly than using all the features. Training stack training is more attractive once the models are used multiple times after being trained. Even so, it may be a challenge if retraining doesn't happen immediately, especially when an adaptive IDS detects new attack methods.

Solving QPSO tasks is done better when several computing platforms and advanced GPUs or TPUs are involved. So, investing money in additional Python tools is valuable in many real-life projects.

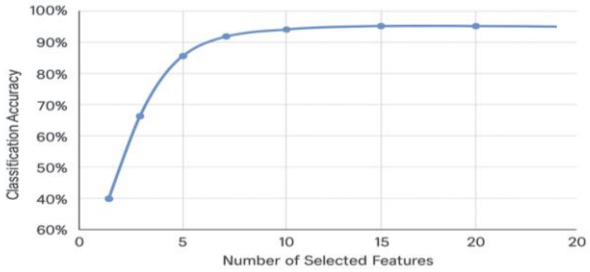

Figure 3: Trade-Off Curve Between Feature Reduction and Classification Accuracy

5.3 Generalizability to Real-World IDS Applications

It is fundamental in IDS research to know how much the suggested strategies generalize outside of research datasets to actual networks used in the world. For this study, we rely on NSL-KDD and CICIDS2017 benchmarks which remain unchanged and miss instances of new and updated attack techniques. Still, using these datasets gives researchers an environment where novel approaches such as QPSO can be repeatedly tested and compared.

Because the approach is designed in a modular style, it is likely to be used broadly. Due to its independence, feature selection can be used in any IDS architecture, regardless of difference in their signatures or representations of data. Furthermore, QPSO often produces a small set of relevant features such as protocol type, connection duration and service type, chosen by experts, improving how easily these algorithms are understood and trusted for use in operations.

At the same time, real data from intrusion detection systems is known for varying attack techniques, encrypted communication and excessive average noise. Because of these complexities, it may be harder for QPSO to fit with the assumptions used for testing. If we consider how conditions change fast in real-world situations, versions of quantum optimization that develop online or step-by-step may be needed to keep up with those scenarios.

5.4 Limitations of the Current Study

Though the results seem positive, we need to recognize a number of limitations. First, the computational requirements of QPSO stand out as the most important factor. Even though the algorithm converges well, choosing superior features and works effectively, the long training time can still be a challenge for organizations without significant computing resources, including SMEs and IDS edge deployments.

My research is affected by a second issue, as well: the dependence on a particular dataset. Widely accepted as standards, these two datasets do not reflect the rich variety often found in actual network traffic. Interestingly, their lack of change over time could result in poor estimates and excessive fit to the data. Moreover, the split of classes in NSL-KDD does not properly illustrate the significant low-frequency dangers in today's cyber attacks. It might favor choosing characteristics that are present in the majority-class in the data.

Furthermore, hyperparameter sensitivity is also a major concern. Both the number of particles, the contraction-explansion ratios and the stopping conditions affect greatly how QPSO does its job. If you don't tune your model correctly, you could end up with the wrong combination of features or take more time for the model to learn. Although grid search and empirical methods were applied, using a common hyperparameter optimization approach (such as Bayes optimization) could help the method work more steadily and become easier for users to use.

Still, we do not hear enough about explainability and transparency. Although QPSO improves how well features are detected, it does not explain why some features were chosen or the effect those features have. Because blockchain's inner workings are not fully understood, organizations in finance and healthcare may not be willing to use it for sensitive information.

6. Future Work

Although we have shown that QPSO is successful at selecting features for IDS, both quantum computing and cybersecurity are undergoing rapid progress which offers numerous opportunities for additional exploration.

6.1 Integration with True Quantum Computing

With quantum computer systems maturing and becoming more available, it becomes less difficult to switch from inspired methods to actually using quantum computers. For example, both D-Wave systems and other gate-based quantum computers can address the type of combinatorial optimization issues found in feature selection. By making use of quantum superposition and entanglement, it is possible to find efficient and scalable answers for handling IDS data with many dimensions. Further research ought to investigate if quantum feature selection methods, for instance the Quantum Approximate Optimization Algorithm (QAOA) and Variational Quantum Eigensolver (VQE), can be used in IDS tasks.

6.2 Real-Time IDS Deployment

Work is also underway to fit quantum-inspired feature selection to real-time or online intrusion detection. The majority of existing methods such as the one examined in this work, process data using batch learning. However, cybersecurity in operations keeps pace with the regular emergence of new threats. By dynamically updating a subset of the features in QPSO using streaming data, an IDS could become both faster in response and more reliable. It becomes important to design items for lower time or energy use in IoT security or edge situations.

6.3 Exploring Alternative Quantum-Inspired Algorithms

In addition to QPSO, other quantum-inspired algorithms should be considered for further study. As an example, the QHO model brings a different expected approach that could provide additional benefits. Also, by relying on quantum concepts, Quantum Evolutionary Algorithms (QEA) apply population evolution to IDS optimization which handles several objectives. If you evaluate both variants, you could better understand which one fits cybersecurity applications best.

6.4 Fusion with Deep Learning Models

Integrating quantum strategies in selecting features together with neural networks is at the forefront of new research. Recent success in network traffic analysis has been found using Convolutional Neural Networks (CNNs) and Long Short-Term Memory networks (LSTMs). Training the classifiers on small, selected sets of features produced by QPSO or alike would allow one to speed up learning and better recognize classes. Fusion of QPSO for feature preprocessing with deep neural networks for identifying malicious activities may result in strong, flexible and smart IDS solutions.

Conclusion

Using quantum-inspired optimization for feature engineering was proposed in the Intrusion Detection Systems (IDS) domain in this paper. Having seen how vital feature selection is for IDS models, we used QPSO to find the best set of features within large network traffic datasets. Our goal was to overt these shortcomings of standard feature selection which often stuck to local

solutions instead of global ones, ran slowly and didn't use as many samples.

Testing on both the NSL-KDD and CICIDS2017 datasets indicates that QPSO gets better results for reducing features and for classifying data sets. Because the data used for training was lower in size and more relevant features were picked using QPSO, accuracy, precision, recall, F1-score and processing time were all improved in these classifiers. The findings indicate that using these algorithms makes it easier to spot useful details and still keep the processing simple.

The research also connects advances in quantum computing with more effective cybersecurity. We demonstrated that a computer with just classical technology can still get improvements from using quantum concepts. Cyber dangers are becoming more of a problem right now, so we rely on systems that can quickly if changes are needed.

Based on the findings in this work, new areas for investigation appear promising. Once true quantum feature selection methods are perfected, the results could create greater opportunities with quantum hardware. Moreover, the ability to detect threats as they happen, adhere to changing threats and join forces with neural and deep learning systems seems promising. In general, using quantum-influenced feature engineering is vital for cybersecurity since it allows intrusion detection systems to run faster, more accurately and with greater dependability in rapidly changing environments.

References

1. Han, K. H., & Kim, J. H. (2002). Quantum-inspired evolutionary algorithm for a class of combinatorial optimization. IEEE transactions on evolutionary computation, 6(6), 580-593.
2. https://doi.org/10.1109/TEVC.2002.804320
3. Han, K. H., Park, K. H., Lee, C. H., & Kim, J. H. (2001, May). Parallel quantum-inspired genetic algorithm for combinatorial optimization problem. In Proceedings of the 2001 congress on evolutionary computation (IEEE Cat. No. 01TH8546) (Vol. 2, pp. 1422-1429). IEEE.
4. https://doi.org/10.1109/CEC.2001.934358
5. da Cruz, A. A., Vellasco, M. M. B. R., & Pacheco, M. A. C. (2006, July). Quantum-inspired evolutionary algorithm for numerical optimization. In 2006 IEEE International Conference on Evolutionary Computation (pp. 2630-2637). IEEE.
6. https://doi.org/10.1109/CEC.2006.1688637
7. Duong, T. Q., Nguyen, L. D., Narottama, B., Ansere, J. A., Van Huynh, D., & Shin, H. (2022). Quantum-inspired real-time optimization for 6G networks: Opportunities, challenges, and the road ahead. IEEE Open Journal of the Communications Society, 3, 1347-1359.
8. https://doi.org/10.1109/OJCOMS.2022.3195219
9. Ganesan, V., Sobhana, M., Anuradha, G., Yellamma, P., Devi, O. R., Prakash, K. B., &Naren, J. (2021). Quantum inspired meta-heuristic approach for optimization of genetic algorithm. Computers & Electrical Engineering, 94, 107356. https://doi.org/10.1016/j.compeleceng.2021.107356
10. Meng, K., Wang, H. G., Dong, Z., & Wong, K. P. (2009). Quantum-inspired particle swarm optimization for valve-point economic load dispatch. IEEE transactions on power systems, 25(1), 215-222.
11. https://doi.org/10.1109/TPWRS.2009.2030359
12. https://onlinelibrary.wiley.com/authored-by/Kochenberger/Gary
13. Soleimanpour-Moghadam, M., Nezamabadi-Pour, H., &Farsangi, M. M. (2014). A quantum inspired gravitational search algorithm for numerical function optimization. Information Sciences, 267, 83-100.https://doi.org/10.1016/j.ins.2013.09.006
14. Li, J., Cheng, K., Wang, S., Morstatter, F., Trevino, R. P., Tang, J., & Liu, H. (2017). Feature selection: A data perspective. ACM computing surveys (CSUR), 50(6), 1-45.
15. https://doi.org/10.1145/3136625
16. Venkatesh, B., &Anuradha, J. (2019). A review of feature selection and its methods. Cybern. Inf. Technol, 19(1), 3-26.
17. Chandrashekar, G., &Sahin, F. (2014). A survey on feature selection methods. Computers & electrical engineering, 40(1), 16-28.
18. https://doi.org/10.1016/j.compeleceng.2013.11.024
19. Jović, A., Brkić, K., &Bogunović, N. (2015, May). A review of feature selection methods with applications. In 2015 38th international convention on information and communication technology, electronics and microelectronics (MIPRO) (pp. 1200-1205). Ieee.https://doi.org/10.1109/MIPRO.2015.7160458
20. Kira, K., & Rendell, L. A. (1992). A practical approach to feature selection. In Machine learning proceedings 1992 (pp. 249-256). Morgan Kaufmann. https://doi.org/10.1016/B978-1-55860-247-2.50037-1