Detecção de anomalias em redes de computadores utilizando Computação Quântica

Mateus Komarchesqui[1], **Mario Lemes Proença Jr**[1]

[1]Departamento de Computação – Universidade Estadual de Londrina (UEL)
Caixa Postal 10.011 – CEP 86057-970 – Londrina – PR – Brasil

mateus.komarchesqui@uel.br, proenca@uel.br

Abstract. *Given the widespread use of computer networks and the potential exposure of devices and data, which can serve as a catalyst for attacks, this work aims to develop a system capable of detecting potential threats through the analysis of network traffic. Over the years, various implementations of Network Intrusion Detection Systems have used Machine Learning within the scope of classical computing. Even with complex Deep Learning models, the discussion about network intrusion remains open. With this in mind, this work aims to study and implement a classic-quantum Hybrid Machine Learning model, highlighting the specifics of this new paradigm and exploring its feasibility in the proposed context.*

Resumo. *Dada a ampla aplicação das redes de computadores e o potencial de exposição de dispositivos e dados, o que pode servir como catalisador para ataques, este trabalho tem como objetivo desenvolver um sistema capaz de detectar possíveis ameaças através da análise do tráfego de rede. Ao longo dos anos, diversas implementações de Sistemas de Detecção de Intrusão de Rede utilizaram Aprendizado de Máquina no âmbito da computação clássica. Mesmo com modelos complexos de Aprendizado Profundo, a discussão acerca de intrusão de rede continua em aberto. Tendo isso em vista, almeja-se com este trabalho estudar e implementar um modelo de Aprendizado de Máquina Híbrido clássico-quântico, mostrando as particularidades desse novo paradigma e explorando sua viabilidade no contexto proposto.*

1. Introdução

Com a democratização do acesso às redes e aos computadores pessoais, sejam *Desktops*, telefones celulares, *gadgets* inteligentes, entre outros, praticamente todos os serviços do cotidiano traçaram uma relação inextricável com a rede. Seu uso é evidenciado desde a navegação na internet, envio de mensagens, acesso a entretenimento até ensino a distância, reuniões virtuais e *e-commerce* [35], [66].

Visto essa alta adesão ao uso da rede e, consequentemente, a exposição de dispositivos e usuários, ataques com diversas motivações ocorrem [29]. Ataques causam ou aproveitam-se de falhas, comprometendo a integridade, disponibilidade e confidencialidade do que trafega ou é armazenado em rede, podendo causar perdas substanciais e irreparáveis [13]. Essas falhas podem surgir fisicamente, por software ou por intervenção humana [29].

O comportamento da rede é alterado uma vez que uma falha ocorre ou é explorada por um ataque, gerando uma anormalidade no fluxo de pacotes. Essa anormalidade é

denominada anomalia. Ataques, por sua vez, são atividades anômalas promovidas por agentes maliciosos mal-intencionados [19].

Uma abordagem para a detecção desses ataques amplamente difundida no meio científico é o chamado Sistema de Detecção de Intrusão de Rede, do inglês *Network Intrusion Detection System* (NIDS) [47], [19], [26]. Um NIDS observa o tráfego da rede a procura de indícios de comportamento anômalo, alertando os administradores da rede, os quais tomam as medidas cabíveis para mitigar o problema. Esses sistemas são implementados utilizando modelos de Aprendizado de Máquina, podendo variar desde Aprendizado Profundo [17], [60], até algoritmos mais simples denominados de Aprendizado Raso [65], [27].

Antes até da invenção o computador pessoal, Peter Shor propôs um algoritmo quântico capaz de fatorar números grandes de maneira exponencialmente mais veloz que os computadores tradicionais [18]. Apesar da proposta ser interessante e inovadora, dela falou-se pouco, uma vez que não havia sequer projeto de um computador quântico, muito menos a possibilidade de implementar esse algoritmo [39]. Nos últimos anos, no entanto, a cena da computação quântica mudou. Empresas como *Google* e *IBM* têm investido em larga escala no desenvolvimento desses dispositivos.

Tendo em vista a grande capacidade computacional e potencial supremacia quântica sobre o paradigma tradicional, a computação quântica tem despertado um crescente interesse na comunidade científica [21], [48]. O tópico foi inundado de questionamentos, desde a sobrevivência dos computadores clássicos como conhecemos até a segurança da criptografia contemporânea. Dessa maneira, a fim de tirar proveito dos benefícios dessa nova abordagem, modelos de Aprendizado de Máquina com aperfeiçoamento quântico, o *Quantum Enhanced Machine Learning*, têm sido empregados para diversas tarefas [20], [10], [59], inclusive a detecção de intrusão [46], [25], [34].

Até mesmo com o uso de abordagens clássicas mais complexas de Aprendizado Profundo como *Generative Adversarial Network* (GAN) [43], *Long Short-Term Memory* (LSTM) [42] e *Convolutional Neural Network* (CNN) [14], o problema de detecção de intrusão continua uma discução em aberto [19]. Motivado por esse fato, este trabalho propõe-se a estudar um modelo de aprendizado de máquina híbrido clássico-quântico no contexto de NIDS.

Este documento está organizado da seguinte maneira: A Seção 2 apresenta os conceitos, métodos, técnicas e revisão do estado da arte necessários para a elaboração do sistema proposto. A Seção 3 apresenta o objetivo a ser alcançado uma vez que o desenvolvimento do proposto seja concluído. A Seção 4 descreve como os objetivos serão atingidos fazendo uso da fundamentação teórico-metodológica e a revisão do estado da arte. A Seção 5 apresenta o cronograma de execução das atividades citadas na seção anterior. Finalmente, na Seção 6 serão descritas as contribuições do trabalho no avanço e consolidação dos conhecimentos dos leitores.

2. Fundamentação Teórico-Metodológica e Estado da Arte

2.1. Anomalias de Rede

Ao observar o meio, neste caso o tráfego da rede, pode-se discernir padrões recorrentes e comportamentos habituais com base nas características primitivas dos dados [53].

Uma análise sobre as observações possibilita a detecção de desvios notáveis nas características, que frequentemente indicam a presença de anomalias. Existem diversos tipos de anomalias de rede, com causas e características únicas [19].

Sendo assim, opta-se pela coleta de dados que consegue capturar mais evidentemente os vestígios de ocorrência das anomalias alvo do Sistema de Detecção de Intrusão. Os dados de tráfego de rede podem ser coletados em diferentes formatos, como *IP Flow*(Fluxo IP), *SNMP* e *TCP dump*.

2.1.1. Detecção de Anomalias de Rede

Os Sistemas de Detecção de Intrusão de Rede, *Network Intrusion Detection System* (NIDS), são uma das soluções mais aceitas para a detecção de anomalias de rede no meio científico. Sua função é reportar qualquer tráfego com traços anormais ao administrador de rede [1], funcionando como um complemento para o *firewall*.

Os ataques estão em constante evolução e concepção [31], dificultando sua detecção. Dessa maneira, além da agilidade na detecção de uma anomalia [15], o NIDS deve ser capaz de identificar anomalias nunca antes vistas. Para isso, existem duas principais implementações de NIDS, categorizadas de acordo com a estratégia utilizada para a detecção [1], [70], [44]. Essas são:

- Baseado em Assinatura: Armazena em um banco de dados os padrões de anomalias já conhecidos e tenta sempre identificar algum desses padrões no tráfego de rede [31]. Devido ao fato de gerar alertas apenas quando uma anomalia for detectada, esse método gera menos falsos positivos [19] e é mais eficiente em identificar anomalias conhecidas. No entanto, anomalias não conhecidas não são detectadas [44].
- Baseado em Anomalia: Constrói um modelo que representa o tráfego normal da rede utilizando dados históricos [19]. O NIDS compara de forma constante o comportamento atual do tráfego da rede com o comportamento considerado normal o qual foi treinado. Isso leva à detecção de anomalias sempre que o comportamento atual difere do esperado como padrão. Essa abordagem possibilita a identificação de anomalias que ainda não foram observadas [19], [44].

A abordagem mais utilizada na literatura é a Baseada em Anomalia e é a que será implementada neste trabalho.

Desde 2004, o grupo de pesquisa ORION da Universidade Estadual de Londrina tem contribuído para o estudo e implementação de Sistemas de Detecção de Intrusão eficientes e flexíveis. Diversos trabalhos foram publicados pelo grupo ao longo dos anos e citados por outros autores acerca da segurança em redes, desde uma revisão detalhada da literatura e da fundamentação teórica [19] até variadas abordagens para detecção de anomalias na abordagem computacional clássica [50], [22], [56], [12], [14], [42], [43], [55], [32], [4]. Além disso, trabalhos como [51] e [49] contribuem de maneira direta para o gerenciamento da rede, sendo cruciais para a área do conhecimento.

A seguir, é apresentada uma análise com dados fictícios para ilustrar uma anomalia. A onda tem seu comportamento padrão no plano cartesiano e no ponto vermelho

destoa dos demais pontos, sendo caracterizado como um ponto anômalo e consequentemente alvo do NIDS.

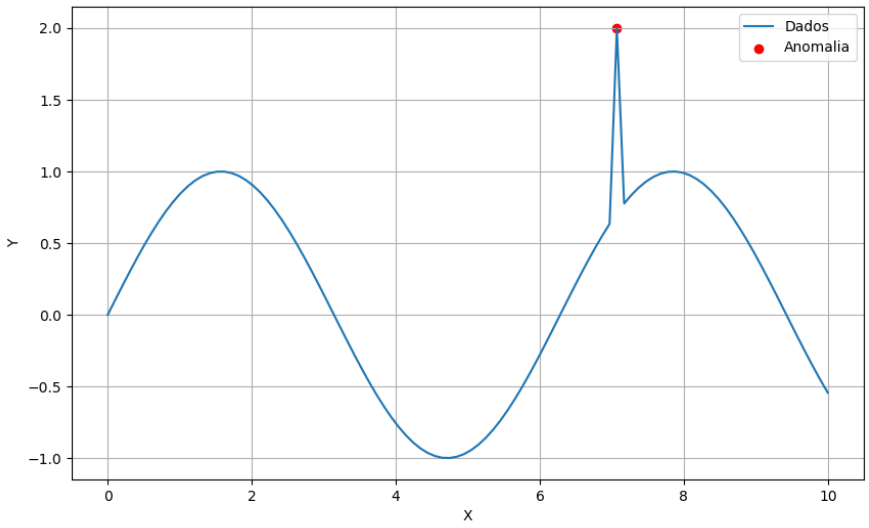

Figura 1. Exemplo de anomalia

2.2. Aprendizado de Máquina

O Aprendizado de Máquina, *Machine Learning* (ML), é uma subárea da Inteligência Artificial, *Artificial Inteligence* (AI). Essa solução computacional utiliza um conjunto de dados base para treinar um modelo que tem por objetivo ser capaz de fazer previsões sobre os dados que o alimentam [2], distintos dos utilizados no treinamento. O *Machine Learning* vem para suprir a necessidade computacional de automatizar a análise e interpretação de grandes volumes de dados complexos, tornando possível identificar padrões e relações que seriam difíceis ou impossíveis de serem percebidos por meio de métodos tradicionais [36].

Pode-se exemplificar a superioridade do ML por meio da aplicação apresentada no artigo [63]. Nele, é exposto o problema: identificar e classificar vida animal capturada por armadilhas fotográficas. Utilizando um modelo treinado com imagens de vida animal, foi possível automatizar o processo de identificação e classificação de novas fotografias com uma precisão notável, tarefa que seria impossível de ser realizada com algoritmos tradicionais devido à complexidade e variabilidade das imagens.

O aprendizado pode ser classificado em três categorias principais, cujas aplicações estão diretamente relacionadas ao conjunto de dados de treinamento [23]: supervisionado 2.2.1, semi-supervisionado 2.2.2 e não-supervisionado 2.2.3 [36], [69], [62].

2.2.1. Aprendizado Supervisionado

O aprendizado supervisionado utiliza dados onde cada observação X possui um rótulo Y relacionado capaz de descrevê-lo [68]. Dessa maneira, o objetivo do modelo que uti-

liza o aprendizado supervisionado é mapear uma observação de entrada X para um Y' satisfatoriamente próximo de Y [36].

Essa abordagem pode ser implementada utilizando diversos algoritmo tanto de classificação quanto de regressão [67]. Neste trabalho um modelo híbrido clássico-quântico supervisionado será estudado e implementado para classificar o tráfego de uma rede de computadores como normal ou anômalo.

2.2.2. Aprendizado Semi-supervisionado

Visto que a etapa de rotulação dos dados é custosa e grande parte das observações não carregam consigo rótulos [36], a aplicação do aprendizado semi-supervisionado pode ser interessante, uma vez que usa dados que contenham rótulos juntamente aos dados que não os contém no processo de treinamento [68].

Uma analogia para a melhor compreensão dessa abordagem é utilizada no livro [36], comparando o aprendizado do ser humano ao aprendizado semi-supervisionado:

> The way we learn is similar to the process of semi-supervised learning. A child is supplied with
>
> 1. Unlabeled data provided by the environment. The surroundings of a child are full of unlabeled data in the beginning.
> 2. Labeled data from the supervisor. For example, a father teaches his children about the names (labels) of objects by pointing toward them and uttering their names.

2.2.3. Aprendizado Não-supervisionado

O aprendizado não-supervisionado faz uso de conjuntos de dados sem rotulação. O objetivo dessa abordagem é encontrar estruturas escondidas nos dados. Uma variedade de motivos podem levar os dados a não possuírem rotulação, desde o alto custo e trabalho agregado à rotulação manual até a natureza intrínseca não-rotulada dos dados [36].

Essa abordagem é amplamente utilizada em sistemas de recomendação [5], por exemplo, que permeiam a internet seja em propagandas baseadas em interesses pessoais, sugestões de produtos em plataformas de comércio eletrônico, ou recomendações de conteúdo em serviços de *streaming*.

2.3. Rede Neural

Rede Neural, *Neural Network* (NN), é uma especialização do Aprendizado de Máquina inspirada no cérebro, utilizando elementos chamados de neurônios e suas conexões para efetuar cálculos complexos [36]. Os neurônios são organizados em camadas sequenciais e adjacentes, o que permite a conexão somente entre neurônios de camadas adjacentes. A primeira e última camada são denominadas respectivamente de camada de entrada e de saída. A primeira é responsável por receber uma entrada X proveniente do conjunto de dados. A última representa a saída Y calculada para a entrada X, seja classificação ou regressão. Entre essas camadas existe pelo menos uma camada oculta. A combinação de número de neurônios por camada e número de camadas ocultas constitui a arquitetura da NN, permitindo inúmeras variações de implementações [67].

2.4. Aprendizado Profundo

O Aprendizado Profundo, *Deep Learning* (DL), é uma especialização mais potente da Rede Neural, sendo denominada Rede Neural Profunda, *Deep Neural Network* (DNN), pois implementa múltiplas camadas ocultas entre a camada de entrada e a de saída [1], [23], [31]. Por esse motivo, a DNN é capaz de performar modelagens mais complexas que a NN [1], [61], solucionando problemas mais elaborados em detrimento de maior uso do poder computacional. O Aprendizado Profundo requer um número maior de observações para ser treinado em comparação ao Aprendizado de Máquina, utilizando as características dos dados para se auto-ajustar [31].

Uma Rede Neural Profunda pode ser classificada como [1]:

Discriminativa	Generativa	Híbrida
Aprendizado Supervisionado	Aprendizado Não-supervisionado	Combinação de Ambos

Tabela 1. Tipos de DNN.

2.5. Rede Adversária Generativa

A Rede Adversária Generativa, *Generative Adversarial Network* (GAN), é uma abordagem de Aprendizado Profundo híbrido, como exposto em 1, baseada na Teoria dos Jogos. Essa é composta por duas Redes Neurais internas que competem entre si, onde uma NN gera dados sintéticos e a outra classifica os seus dados de entrada como sintéticos (gerados) ou orgânicos (advindos do conjunto de dados) [33], [40], [54].

A Rede Neural responsável por sintetizar dados é chamada de gerador e a responsável por distinguir dados reais de dados gerados é chamada de Discriminador. O objetivo do gerador é enganar o Discriminador e do Discriminador discernir o que lhe é alimentado.

Visto que a GAN é uma abordagem generativa, uma de suas principais aplicações é a geração de dados. Dessa maneira, o treinamento desse modelo tem como objetivo criar um gerador capaz de enganar completamente o discriminador, gerando dados muito similares aos reais [40].

As Redes Generativas Adversárias têm sido amplamente empregadas na área de visão computacional, seja convertendo fotografias tiradas durante a noite para simular dia [72], seja gerando imagens realistas de alta qualidade a partir de descrição textual [73]. Esse modelo de Aprendizado Profundo têm se mostrado útil na detecção de anomalias [30], [57], e, consequentemente, na implementação se Sistemas de Detecção de Intrusão.

2.6. Computação Quântica

Muita incerteza tem permeado o tema "Computação Quântica". Alguns dizem ser o fim da computação como conhecemos, o fim da criptografia, mas ainda estamos muito distantes de substituir os computadores clássicos [21], [39].

A seguir estão explicitadas algumas das motivações para a pesquisa na área, as principais diferenças em relação à computação clássica, o atual estado dos computadores quânticos e uma introdução ao Aprendizado de Máquina Híbrido.

2.6.1. O Fim da Lei de Moore?

Desde 1965 os computadores tiveram sua capacidade de processamento descrita segundo a lei de Moore [38], a qual afirma que a cada dois anos o poder de processamento de um dispositivo dobra [37]. Essa preditiva que se mostrou válida desde *chips* integrados com 100 transistores até os dias atuais, onde bilhões de transistores compõem um único *chip* [39]. Dessa maneira, autores como [71] afirmaram com plena convicção que a evolução tecnológica segue um caminho razoavelmente previsível. E que, apesar das previsões do eventual fim da Lei de Moore por alguma barreira tecnológica ou científica, os engenheiros e cientistas têm encontrado formas de contornar essas barreiras, prolongando indeterminadamente a vigência dessa Lei.

Essas afirmações, no entanto, contradizem a física moderna, que garante um limite absoluto que a ciência e engenharia consegue atingir. O princípio da Incerteza de Heisenberg postula que há uma limitação da precisão com que podemos medir certas propriedades de partículas subatômicas [11]. Ainda, o físico Stephen Hawking em 2005, durante sua visita à Intel, afirmou que a velocidade da luz e a natureza atômica da matéria seriam os limites fundamentais para a microeletrônica.

De maneira geral, o fim ou não da Lei de Moore é uma discussão em aberto, mas é inegável que a incerteza da sua continuidade foi crucial para direcionar os holofotes em direção à computação quântica.

2.6.2. O Fim da Tese Estendida de Church-Turing

Em 1993 Berstein et al. mostrou que os computadores quânticos poderiam violar a Tese Estendida de Church-Turing [8], que afirma que qualquer "modelo razoável"de computação pode ser eficientemente simulado em um modelo padrão, como uma Máquina de Turing, uma Máquina de Acesso Aleatório ou um autômato celular.

Apenas um ano depois, em 1994, Peter Shor mostrou um algoritmo capaz de resolver um problema exponencialmente mais rápido que um computador clássico. O chamado Algoritmo de Shor, é um exemplo prático de fatoração de números grandes onde é confirmada a tese apresentada em 1993 por Berstein et al. [18].

Por mais que esse algoritmo fosse interessante para o período, nenhum cientista tinha sequer ideia de como construir um computador quântico. Nos dias de hoje, no entanto, não apenas é possível implementar o Algoritmo de Shor[0] , mas também executá-lo em simulações ou computadores quânticos reais. É importante levar em conta que a implementação genérica desse está limitada pela disponibilidade de *qubits*.

2.6.3. O Novo Paradigma

Os computadores clássicos possuem circuitos integrados contendo bilhões de transistores que operam sobre os dígitos binários (*bits*), que por sua vez podem assumir valores de-

[0] O Algoritmo de Shor é um algoritmo de tempo polinomial que usa, como mostrado em [6], $2n + 3$ *qubits* para fatorar um número inteiro de n *bits*.

terminísticos 0 ou 1. Através da manipulação desses bits os dispositivos são capazes de representar informações, operações e, em larga escala, aplicativos e serviços [39].

Um computador quântico também representa informação em uma espécie de *bit*, o *qubit*. O *qubit*, abreviação para *Quantum Bit*, também pode assumir o valor de 0 ou 1, mas não fica limitado a isso. Essa unidade de dados pode ficar em um estado de superposição, onde é 0 e 1 ao mesmo tempo. Dessa maneira, um sistema com múltiplos *qubits* pode estar em todos os estados binários possíveis, levando em conta a quantidade de dígitos binários, ao mesmo tempo [24], [3], [16], [39]. Ao longo de um algoritmo quântico, manipulam-se as distribuições probabilísticas desses estados de superposição. Devido à natureza probabilística desses algoritmos, esses são repetidos um número de vezes, a fim de manter um resultado relativamente consistente [59]. Esse fenômeno é conhecido como interferência quântica e é fundamental para o poder de processamento dos computadores quânticos [9], [39].

Os *qubits*, no entanto, são sensíveis a interferências do ambiente, o que pode levar a erros no processamento. Para mitigar esse problema, os computadores quânticos utilizam um processo chamado correção de erros quânticos. Nele, os qubits são redundantes para tentar alcançar uma precisão maior nos cálculos [41]. É natural que um *qubit* decaia ao longo de sua manipulação, principalmente ao ser aplicado em circuitos maiores e mais complexos, perdendo o estado de superposição em que estava, invalidando seu uso [64].

Além disso, uma propriedade importante dos *qubits* é a chamada emaranhamento, do inglês *entanglement*. Quando *qubits* estão emaranhados, o estado de um *qubit* não pode ser descrito independentemente do estado de outros *qubits* emaranhados com ele [64], [28]. Essa característica é explorada em algoritmos quânticos num geral, assim como no Algoritmo de Shor [18].

É importante destacar que nem todos os problemas podem ser resolvidos de forma mais eficiente com computadores quânticos. Eles se destacam na resolução de problemas inerentemente quânticos, inteligência artificial e criptografia. Para as demais tarefas esses computadores podem não ser atraentes [39].

2.6.4. Noisy Intermediate-Scale Quantum Era

Atualmente estamos na denominada *Noisy Intermediate-Scale Quantum Era* (NISQ Era), termo usado para expressar a situação atual dos computadores quânticos, de Escala Intermediária e com Ruídos [48], [21], [9]. A dita ”vantagem quântica”só pode ser atingida em sua completude com alta disponibilidade de *qubits* e menor taxa de erros devido à decaimentos [21], sendo assim, a tecnologia que temos até então não é matura o suficiente.

A pesquisa e estudo na área é promissora, como destaca o autor John Preskill, em 2018, sobre a então futura computação quântica [48]:

> NISQ devices will be useful tools for exploring many-body quantum physics, and may have other useful applications, but the 100-qubit quantum computer will not change the world right away — we should regard it as a significant step toward the more powerful quantum technologies of the future. Quantum technologists should continue to strive for more accurate quantum gates and, eventually, fully fault-tolerant quantum computing.

Serviços pagos da IBM já contam com *chips* quânticos de 127 *qubits*, no entanto ainda são muito propensos a ruídos. O plano grátis da empresa conta com *chips* de 8 *qubits* e um *runtime* limitado mensalmente. Outra alternativa é a simulação, encontrada em bibliotecas como *Pennylane*, *Cirq* e até mesmo *Qiskit*, trazendo implementações em *Python*.

2.6.5. Aprendizado de Máquina Híbrido

Algoritmos quânticos utilizam da mecânica quântica para expressar sub-rotinas de maneira eficiente, traduzindo métodos clássicos para essa nova abordagem [59]. No caso do Aprendizado de Máquina Híbrido, usa-se tanto a computação clássica como quântica, onde uma parcela computacionalmente custosa e complexa é delegada para um dispositivo quântico [7], [58]. Esse aprendizado pode ser aplicado a dados inerentemente quânticos [39] ou de natureza quântica, mirando apenas na alta capacidade de processamento dos computadores quânticos. Este trabalho propõe-se a estudar e classificar um problema de natureza clássica, onde os dados são referentes a coleta de fluxos IP de uma rede de computadores, tirando proveito do paradigma quântico.

O modelo proposto neste trabalho é o *Quantum Support Vector Machine* (QSVM), uma derivação do *Support Vector Machine* (SVM) clássico, utilizando um *kernel* quântico. O SVM é um modelo de Aprendizado de Máquina Raso, utilizado para discriminação linear. O intuito do SVM é determinar qual o hiperplano que melhor separa as classes de dados no espaço [59], [45].

Visto que os dados em sua grande maioria não são linearmente separáveis ou sequer disjuntos, faz-se necessário mapear os dados de entrada para dimensões maiores. Dessa maneira, o melhor hiperplano é aquele que consegue determinar, de maneira geral, a maior distância entre os dados que separa (*maximum-margin*) [2], [45] ou ser mais flexível para os valores discrepantes com a chamada *soft-margin* [45]. A margem é calculada do hiperplano em relação os chamados Vetores de Suporte, *Support Vectors*, os dados mais próximos espacialmente à borda de cada classe [59], [2].

Os SVMs possuem o chamado kernel, uma função capaz de projetar os dados de entrada em dimensões maiores a fim de determinar uma separação linear para os mesmos, podendo ser linear, polinomial, *radial basis function* ou sigmoid [45]. O kernel pode ser implementado, ainda, de maneira pré-computada, na forma de matriz de correlação. Nessa abordagem, o cálculo de correlação dos dados é determinado pelo produto escalar dos seus pares [52]. Calcular essa matriz, no entanto, é computacionalmente custoso e delegar o seu cálculo a um computador quântico pode tornar o processo mais eficiente, como será estudado neste trabalho.

3. Objetivos

Este trabalho tem por objetivo a pesquisa e implementação de uma solução de detecção de anomalias em redes de computadores utilizando a Computação quântica.

4. Procedimentos metodológicos/Métodos e técnicas

Um estudo geral sobre a computação quântica será conduzido. Como funcionam esses novos dispositivos e como o novo paradigma computacional é aplicado no contexto de

Aprendizado de Máquina. Após o estudo, um modelo híbrido de Aprendizado de Máquina será desenvolvido para detectar anomalias, implementando um Sistema de Detecção de Intrusão de Rede. O sistema será treinado e testado utilizando o conjunto de dados do grupo ORION da Universidade Estadual de Londrina, no formato de Fluxo IP coletado pela ferramenta Mininet.

5. Cronograma de Execução

Este trabalho teve sua execução dividida em 9 atividades, buscando a organização descrita na tabela 2.

Atividades:

1. Levantamento bibliográfico;
2. Testes de viabilidade;
3. Estudo da base matemática e física;
4. Estudo de Aprendizado de Máquina aplicado a NIDS;
5. Implementação do modelo de ML híbrido e suas otimizações;
6. Implementação de modelo de ML clássico similar;
7. Testes, comparação e ajuste dos modelos;
8. Escrita do TCC na versão preliminar;
9. Escrita do TCC na versão banca examinadora;

Tabela 2. Cronograma de Execução

	ago	set	out	nov	dez	jan	fev	mar	abr	mai
Atividade 1	●	●								
Atividade 2	●									
Atividade 3	●	●	●							
Atividade 4		●	●							
Atividade 5	●		●	●						
Atividade 6		●		●	●					
Atividade 7						●	●	●		
Atividade 8		●	●	●	●					
Atividade 9						●	●	●	●	●

6. Contribuições e/ou Resultados esperados

Espera-se desenvolver uma aplicação do mundo real utilizando o novo paradigma da computação quântica, capaz de detectar anomalias no contexto de redes de computadores, implementando um Sistema de Detecção de Intrusão de Rede.

7. Espaço para assinaturas

Londrina, *18 de Setembro de 2023*.

Mateus Komarchesqui
Assinado de forma digital por Mateus Komarchesqui
Dados: 2023.09.13 17:31:45 -03'00'

Aluno

Orientador

Referências

[1] Arwa Aldweesh, Abdelouahid Derhab, and Ahmed Z Emam. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189:105124, 2020.

[2] Ethem Alpaydin. *Introduction to machine learning*. MIT press, 2020.

[3] Pedram Khalili Amiri. Quantum computers. *IEEE Potentials*, 21(5):6–9, 2003.

[4] Marcos VO Assis, Luiz F Carvalho, Jaime Lloret, and Mario L Proença Jr. A gru deep learning system against attacks in software defined networks. *Journal of Network and Computer Applications*, 177:102942, 2021.

[5] Sagarika Bakshi, Alok Kumar Jagadev, Satchidananda Dehuri, and Gi-Nam Wang. Enhancing scalability and accuracy of recommendation systems using unsupervised learning and particle swarm optimization. *Applied Soft Computing*, 15:21–29, 2014.

[6] Stephane Beauregard. Circuit for shor's algorithm using 2n+ 3 qubits. *arXiv preprint quant-ph/0205095*, 2002.

[7] Marcello Benedetti, John Realpe-Gómez, Rupak Biswas, and Alejandro Perdomo-Ortiz. Quantum-assisted learning of hardware-embedded probabilistic graphical models. *Physical Review X*, 7(4):041052, 2017.

[8] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, pages 11–20, 1993.

[9] Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Heimonen, Jakob S Kottmann, Tim Menke, et al. Noisy intermediate-scale quantum algorithms. *Reviews of Modern Physics*, 94(1):015004, 2022.

[10] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549(7671):195–202, 2017.

[11] Paul Busch, Teiko Heinonen, and Pekka Lahti. Heisenberg's uncertainty principle. *Physics reports*, 452(6):155–176, 2007.

[12] Luiz F Carvalho, Gilberto Fernandes, Joel JPC Rodrigues, Leonardo S Mendes, and Mario Lemes Proença. A novel anomaly detection system to assist network management in sdn environment. In *2017 IEEE international conference on communications (ICC)*, pages 1–6. IEEE, 2017.

[13] Roza Dastres and Mohsen Soori. A review in recent development of network threats and security measures. *International Journal of Information Sciences and Computer Engineering*, 2021.

[14] Marcos VO de Assis, Luiz F Carvalho, Joel JPC Rodrigues, Jaime Lloret, and Mario L Proença Jr. Near real-time security system applied to sdn environments in iot networks using convolutional neural network. *Computers & Electrical Engineering*, 86:106738, 2020.

[15] Marcos VO De Assis, Matheus P Novaes, Cinara B Zerbini, Luiz F Carvalho, Taufik Abrãao, and Mario L Proença. Fast defense system against attacks in software defined networks. *IEEE Access*, 6:69620–69639, 2018.

[16] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[17] Bo Dong and Xue Wang. Comparison deep learning method to traditional methods using for network intrusion detection. In *2016 8th IEEE International Conference on Communication Software and Networks (ICCSN)*, pages 581–585, 2016.

[18] Artur Ekert and Richard Jozsa. Quantum computation and shor's factoring algorithm. *Reviews of Modern Physics*, 68(3):733, 1996.

[19] Gilberto Fernandes, Joel JPC Rodrigues, Luiz Fernando Carvalho, Jalal F Al-Muhtadi, and Mario Lemes Proença. A comprehensive survey on network anomaly detection. *Telecommunication Systems*, 70:447–489, 2019.

[20] David Peral García, Juan Cruz-Benito, and Francisco José García-Peñalvo. Systematic literature review: Quantum machine learning and its applications. *arXiv preprint arXiv:2201.04093*, 2022.

[21] Ilie-Daniel Gheorghe-Pop, Nikolay Tcholtchev, Tom Ritter, and Manfred Hauswirth. Quantum devops: Towards reliable and applicable nisq quantum computing. In *2020 IEEE Globecom Workshops (GC Wkshps*, pages 1–6, 2020.

[22] Anderson Hiroshi Hamamoto, Luiz Fernando Carvalho, Lucas Dias Hiera Sampaio, Taufik Abrão, and Mario Lemes Proença Jr. Network anomaly detection system using genetic algorithm and fuzzy logic. *Expert Systems with Applications*, 92:390–402, 2018.

[23] William Grant Hatcher and Wei Yu. A survey of deep learning: Platforms, applications and emerging research trends. *IEEE Access*, 6:24411–24432, 2018.

[24] Tony Hey. Quantum computing: an introduction. *Computing & Control Engineering Journal*, 10(3):105–112, 1999.

[25] Maxim Kalinin and Vasiliy Krundyshev. Security intrusion detection using quantum machine learning techniques. *Journal of Computer Virology and Hacking Techniques*, 19(1):125–136, 2023.

[26] Farrukh Aslam Khan, Abdu Gumaei, Abdelouahid Derhab, and Amir Hussain. A novel two-stage deep learning model for efficient network intrusion detection. *IEEE Access*, 7:30373–30385, 2019.

[27] Daniel E Kim and Mikhail Gofman. Comparison of shallow and deep neural networks for network intrusion detection. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 204–208. IEEE, 2018.

[28] Franck Laloë. *Quantum Entanglement*, page 189–222. Cambridge University Press, 2 edition, 2019.

[29] S. Latha and Sinthu Janita Prakash. A survey on network attacks and intrusion detection systems. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pages 1–7, 2017.

[30] Chang-Ki Lee, Yu-Jeong Cheon, and Wook-Yeon Hwang. Studies on the gan-based anomaly detection methods for the time series data. *IEEE Access*, 9:73201–73215, 2021.

[31] Sang-Woong Lee, Mokhtar Mohammadi, Shima Rashidi, Amir Masoud Rahmani, Mohammad Masdari, Mehdi Hosseinzadeh, et al. Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review. *Journal of Network and Computer Applications*, 187:103111, 2021.

[32] Daniel M Brandão Lent, Matheus P Novaes, Luiz F Carvalho, Jaime Lloret, Joel JPC Rodrigues, and Mario Lemes Proença. A gated recurrent unit deep learning model to detect and mitigate distributed denial of service and portscan attacks. *IEEE Access*, 10:73229–73242, 2022.

[33] Yanchun Li, Qiuzhen Wang, Jie Zhang, Lingzhi Hu, and Wanli Ouyang. The theoretical research of generative adversarial networks: an overview. *Neurocomputing*, 435:26–41, 2021.

[34] Jin-Min Liang, Shu-Qian Shen, Ming Li, and Lei Li. Quantum anomaly detection with density estimation and multivariate gaussian distribution. *Physical Review A*, 99(5):052310, 2019.

[35] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516, 2012.

[36] Mohssen Mohammed, Muhammad Badruddin Khan, and Eihab Bashier Mohammed Bashier. *Machine learning: algorithms and applications*. Crc Press, 2016.

[37] Gordon Moore. Moore's law. *Electronics Magazine*, 38(8):114, 1965.

[38] Gordon E Moore. Cramming more components onto integrated circuits. *Proceedings of the IEEE*, 86(1):82–85, 1998.

[39] Engineering National Academies of Sciences, Medicine, et al. Quantum computing: progress and prospects. 2019.

[40] Hojjat Navidan, Parisa Fard Moshiri, Mohammad Nabati, Reza Shahbazian, Seyed Ali Ghorashi, Vahid Shah-Mansouri, and David Windridge. Generative adversarial networks (gans) in networking: A comprehensive survey & evaluation. *Computer Networks*, 194:108149, 2021.

[41] Michael A Nielsen and Isaac L Chuang. Quantum computation and quantum information. *Phys. Today*, 54(2):60, 2001.

[42] Matheus P Novaes, Luiz F Carvalho, Jaime Lloret, and Mario Lemes Proenca. Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. *IEEE Access*, 8:83765–83781, 2020.

[43] Matheus P Novaes, Luiz F Carvalho, Jaime Lloret, and Mario Lemes Proença Jr. Adversarial deep learning approach detection and defense against ddos attacks in sdn environments. *Future Generation Computer Systems*, 125:156–167, 2021.

[44] Yazan Otoum and Amiya Nayak. As-ids: Anomaly and signature based ids for the internet of things. *Journal of Network and Systems Management*, 29:1–26, 2021.

[45] Arti Patle and Deepak Singh Chouhan. Svm kernel functions for classification. In *2013 International Conference on Advances in Technology and Engineering (ICATE)*, pages 1–9, 2013.

[46] ED Payares and Juan Carlos Martínez-Santos. Quantum machine learning for intrusion detection of distributed denial of service attacks: a comparative overview. *Quantum Computing, Communication, and Simulation*, 11699:35–43, 2021.

[47] Eduardo HM Pena, Luiz F Carvalho, Sylvio Barbon Jr, Joel JPC Rodrigues, and Mario Lemes Proença Jr. Anomaly detection using the correlational paraconsistent machine with digital signatures of network segment. *Information Sciences*, 420:313–328, 2017.

[48] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[49] M Lemes Proença, Camiel Coppelmans, Mauricio Bottoli, A Alberti, and Leonardo S Mendes. The hurst parameter for digital signature of network segment. In *Telecommunications and Networking-ICT 2004: 11th International Conference on Telecommunications, Fortaleza, Brazil, August 1-6, 2004. Proceedings 11*, pages 772–781. Springer, 2004.

[50] Mario Lemes Proença, Bruno Bogaz Zarpelão, and Leonardo S Mendes. Anomaly detection for network servers using digital signature of network segment. In *Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop (AICT/SAPIR/ELETE'05)*, pages 290–295. IEEE, 2005.

[51] Mario Lemes Proenca Jr, Gilberto Fernandes Jr, Luiz F Carvalho, Marcos VO de Assis, and Joel JPC Rodrigues. Digital signature to help network management using flow analysis. *International Journal of Network Management*, 26(2):76–94, 2016.

[52] Mathieu Ramona, Gaël Richard, and Bertrand David. Multiclass feature selection with kernel gram-matrix-based criteria. *IEEE Transactions on Neural Networks and Learning Systems*, 23:1611–1623, 2012.

[53] Markus Ring, Sarah Wunderlich, Deniz Scheuring, Dieter Landes, and Andreas Hotho. A survey of network-based intrusion detection data sets. *Computers & Security*, 86:147–167, 2019.

[54] Afia Sajeeda and BM Mainul Hossain. Exploring generative adversarial networks and adversarial training. *International Journal of Cognitive Computing in Engineering*, 3:78–89, 2022.

[55] Gustavo F Scaranti, Luiz F Carvalho, Sylvio Barbon, and Mario Lemes Proença. Artificial immune systems and fuzzy logic to detect flooding attacks in software-defined networks. *IEEE Access*, 8:100172–100184, 2020.

[56] Gustavo Frigo Scaranti, Luiz Fernando Carvalho, Sylvio Barbon Junior, Jaime Lloret, and Mario Lemes Proença Jr. Unsupervised online anomaly detection in software defined network environments. *Expert Systems with Applications*, 191:116225, 2022.

[57] Thomas Schlegl, Philipp Seeböck, Sebastian M Waldstein, Georg Langs, and Ursula Schmidt-Erfurth. f-anogan: Fast unsupervised anomaly detection with generative adversarial networks. *Medical image analysis*, 54:30–44, 2019.

[58] Maria Schuld, Alex Bocharov, Krysta M Svore, and Nathan Wiebe. Circuit-centric quantum classifiers. *Physical Review A*, 101(3):032308, 2020.

[59] Maria Schuld, Ilya Sinayskiy, and Francesco Petruccione. An introduction to quantum machine learning. *Contemporary Physics*, 56(2):172–185, 2015.

[60] Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai, and Qi Shi. A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1):41–50, 2018.

[61] Ajay Shrestha and Ausif Mahmood. Review of deep learning algorithms and architectures. *IEEE access*, 7:53040–53065, 2019.

[62] Nasrin Sultana, Naveen Chilamkurti, Wei Peng, and Rabei Alhadad. Survey on sdn based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*, 12:493–501, 2019.

[63] Michael A Tabak, Mohammad S Norouzzadeh, David W Wolfson, Steven J Sweeney, Kurt C VerCauteren, Nathan P Snow, Joseph M Halseth, Paul A Di Salvo, Jesse S Lewis, Michael D White, et al. Machine learning to classify animal species in camera trap images: Applications in ecology. *Methods in Ecology and Evolution*, 10(4):585–590, 2019.

[64] Barbara M Terhal. Quantum error correction for quantum memories. *Reviews of Modern Physics*, 87(2):307, 2015.

[65] Huiwen Wang, Jie Gu, and Shanshan Wang. An effective intrusion detection framework based on svm with feature augmentation. *Knowledge-Based Systems*, 136:130–139, 2017.

[66] Andrew Whitmore, Anurag Agarwal, and Li Da Xu. The internet of things—a survey of topics and trends. *Information systems frontiers*, 17:261–274, 2015.

[67] Junfeng Xie, F Richard Yu, Tao Huang, Renchao Xie, Jiang Liu, Chenmeng Wang, and Yunjie Liu. A survey of machine learning techniques applied to software defined networking (sdn): Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(1):393–430, 2018.

[68] Yang Xin, Lingshuang Kong, Zhi Liu, Yuling Chen, Yanmiao Li, Hongliang Zhu, Mingcheng Gao, Haixia Hou, and Chunhua Wang. Machine learning and deep learning methods for cybersecurity. *Ieee access*, 6:35365–35381, 2018.

[69] Linli Xu, Martha White, and Dale Schuurmans. Optimal reverse prediction: A unified perspective on supervised, unsupervised and semi-supervised learning. In *Proceedings of the 26th Annual International Conference on Machine Learning*, ICML '09, page 1137–1144, New York, NY, USA, 2009. Association for Computing Machinery.

[70] Zhen Yang, Xiaodong Liu, Tong Li, Di Wu, Jinjiang Wang, Yunwei Zhao, and Han Han. A systematic literature review of methods and datasets for anomaly-based network intrusion detection. *Computers & Security*, 116:102675, 2022.

[71] Mark Yoder and GC Orsak. Engineering: our digital future. 2004.

[72] Bo Yu, Hanting Wei, and Wei Wang. Gan-based day and night image cross-domain conversion research and application. In *2022 11th International Conference of Information and Communication Technology (ICTech))*, pages 230–235, 2022.

[73] Han Zhang, Tao Xu, Hongsheng Li, Shaoting Zhang, Xiaogang Wang, Xiaolei Huang, and Dimitris N Metaxas. Stackgan: Text to photo-realistic image synthesis with stacked generative adversarial networks. In *Proceedings of the IEEE international conference on computer vision*, pages 5907–5915, 2017.