Proposta de projeto: Detecção de Intrusão em Redes com uso de machine learning

Erick Alen Ricioli
Engenharia de Computação
Universidade Tecnológica Federal do Paraná
Cornélio Procópio, Paraná, Brasil
erick.1998@alunos.utfpr.edu.br

Lucas Paschoalick
Engenharia de Computação
Universidade Tecnológica Federal do Paraná
Cornélio Procópio, Paraná, Brasil
paschoalick@alunos.utfpr.edu.br

Luiz Felipe Alves Ferreira
Engenharia de Computação
Universidade Tecnológica Federal do Paraná
Cornélio Procópio, Paraná, Brasil
lferreira.2000@alunos.utfpr.edu.br

Vítor Ângelo Misciato Teixeira*
Engenharia de Computação
Universidade Tecnológica Federal do Paraná
Cornélio Procópio, Paraná, Brasil
vitor.2018@alunos.utfpr.edu.br

I. Introdução e motivação

Com a expansão de funcionalidades da internet atingindo inúmeras indústrias (cinema, e-commerce, jogos, música, alimentos), a internet se tornou uma forma de comércio viável e pouco explorada, sendo cada vez mais usada com esse intuito devido a sua praticidade e rapidez, tanto para as empresas quanto para os consumidores, observando um crescimento de 1500% entre 2012 a 2022 [1].

Neste período, muitas empresas e negócios passaram a operar dentro do ambiente da *internet* e com esses novos agentes surge a necessidade de que as informações que trafegam na rede cheguem ao destino de forma segura, ou seja, sem adulterações e de forma confidencial.

Um problema comum, neste cenário, é a invasão de redes de computadores que pode causar um prejuízo a empresa, afetando tanto a produtividade quanto a imagem dela. Com base nisso, são definidos 5 pilares que a segurança deve garantir, sendo eles: confidenciabilidade da mensagem, integridade da mensagem, autentificação da mensagem, não repúdio da mensagem e identificação do usuário [2].

Buscando evitar esse tipo de situação, uma série de técnicas e ferramentas de prevenção são utilizadas, como é o caso dos *Intrusion Detection Systems* (IDS), ou Sistemas de Detecção de Intrusão. Conforme [3]: "Um IDS é um sistema de software ou hardware que é usado para detectar sinais de atividade maliciosa em uma rede ou um computador individual". As funções de um IDS são divididas entre sensores IDS, que coletam dados em tempo real sobre o funcionamento dos componentes da rede e computadores, e um gerente IDS, que recebe relatórios de sensores.

Existem dois tipos principais, sendo um deles baseado em rede, que monitora uma rede ou um segmento de uma rede, e o outro baseado em *host*, os quais monitoram um único sistema.

O *Network Intrusion Detection System* (NIDS) detecta comportamentos maliciosos baseados em padrões de tráfego e conteúdo, ou seja, faz comparações utilizando os dados dos pacotes da rede. De acordo com [7], a vantagem de usar um NIDS é que além de ser uma abordagem mais econômica, sua resposta é mais rápida, pois seu monitoramento do tráfego é praticamente instantâneo, detectando ataques à medida que ocorrem. Todavia, ele não detecta se os ataques foram bem sucedidos ou não e podem não reconhecer um ataque lançado durante um período de alto tráfego na rede.

O *machine learning*, por sua vez, ajuda na evolução desses sistemas de segurança com base na identificação de padrões - tanto explícitos quanto implícitos - somente com a análise de dados que lhe forem cedidos. Seus algoritmos são diferenciados pela variedade de estilos de aprendizados que podem ser empregados de acordo com a forma de trabalho de cada um [4]. Os aprendizados podem ser classificados em: supervisionados, não-supervisionados e semi-supervisionados.

O aprendizado supervisionado realiza sua captação, como o ser humano, através de uma supervisão realizada por outro ser humano, mostrando quais os dados que se encaixam com as entradas dadas como exemplo. Os dados ficam padronizados de forma explícita e clara, dentro de rótulos já esperados, pois foram pré-determinados [5].

Já o aprendizado não-supervisionado atua de maneira contrária, requerendo do sistema uma decisão própria, a partir de um conjunto de dados predefinidos pelo responsável. Desse modo, o sistema, se bem implementado, pode encontrar padrões implícitos e que não foram identificados anteriormente, podendo levar novas percepções sobre os dados [5].

Além disso, também existe a aprendizagem semi-supervisionada, que mescla os dois tipos citados acima, e a aprendizagem por reforço, que trabalha com o sistema de recompensa e punição [5].

Para se desenvolver um NIDS usando inteligência artificial, é necessário o pré-processamento dos dados, treinamento do

algoritmo e os testes. Vale ressaltar que o tempo de treinamento de um algoritmo de *deep learning* é maior, devido a complexidade de sua estrutura. Quando o modelo é treinado, realiza-se um teste com seu *dataset* - conjunto de dados -, onde ele é avaliado conforme as predições obtidas, onde o tráfego de rede pode atestar um comportamento padrão ou nocivo [6].

Como trata-se de um problema de classificação, existem vários algoritmos que podem ser usados, como, por exemplo: árvores de decisão, KNN, máquina de suporte de vetores, agrupamento k-médias, Redes Neurais Artificiais, métodos com ensemble, dentre outras variações [4].

Portanto, a quantidade de brechas de ataque que um sistema pode fornecer - de maneira involuntária - aumenta concomitantemente, podendo levar muito tempo para ser encontrada por um ser humano. Dessa forma, cresce a motivação da implementação do *machine learning* dentro de um sistema de rede que detecta anomalias dentro do sistema com uma boa eficácia conforme os parâmetros estipulados.

O restante do texto é organizado da seguinte maneira: a seção II apresenta a proposta de intervenção para solucionar os pormenores citados. A seção III mostra as considerações finais, elucidando o objetivo do trabalho, seguido das referências.

II. Proposta

Dado o exposto, o objetivo do trabalho é desenvolver um modelo de *machine learning* que seja capaz de classificar se um fluxo de pacotes em uma rede representa uma ameaça ou não, e, caso represente, qual o tipo específico de ameaça. Assim, a proposta será baseada no problema e solução apresentado por [7], no qual os autores desenvolvem um método de detecção de intrusão com base no *dataset* NSL-KDD, disponibilizado pela *University of New Brunswick* (UNB) e amplamente utilizado em trabalhos na área, criando modelos utilizando algoritmos baseados em árvore para classificação das ameaças.

Logo, a ideia é seguir o mesmo *workflow* proposto pelos autores, mas aplicando uma abordagem diferente em dois aspectos principais: a manipulação e seleção dos atributos do NSL-KDD e a escolha dos algoritmos utilizados para classificação. Para isso, será feita a análise exploratória e manipulação dos dados utilizando a linguagem *Python*, tendo como base o que é chamado *PyData Stack*, composto pelas bibliotecas *pandas, numpy, sklearn, matplotlib e SciPy*. Na Figura 1 é apresentado o *workflow* proposto por [7].

Ao final, pretende-se entregar um arquivo do *Jupyter Notebook* contendo todo o passo a passo realizado durante o processo de desenvolvimento, bem como os arquivos contendo os modelos criados.

Durante a realização do projeto também será utilizado o *GitHub* como repositório dos arquivos e trabalho colaborativo. A comunicação e planejamento será feita via *WhatsApp*.

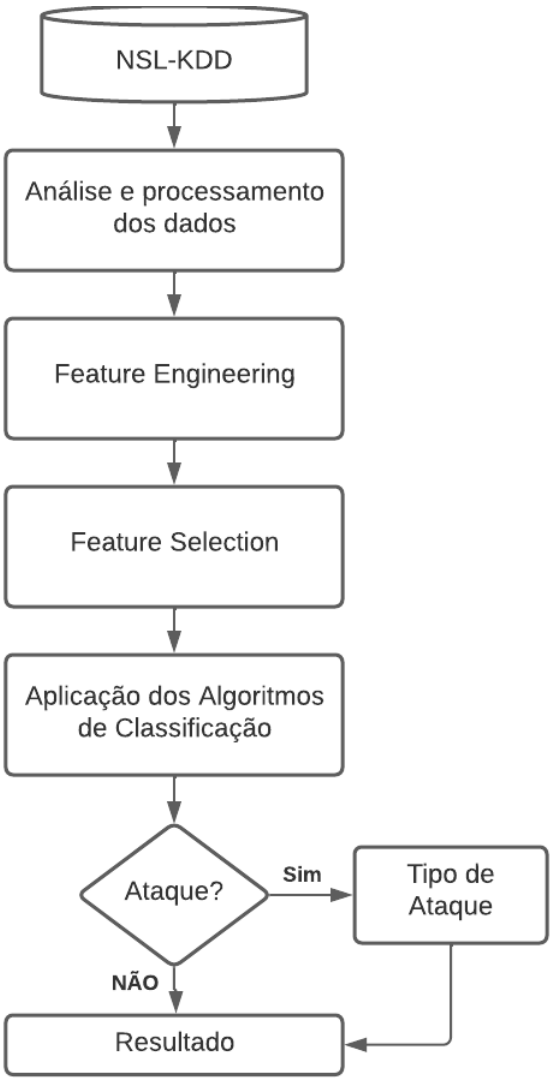

Figura 1. *Workflow* do projeto.

III. Considerações finais

A proposta do trabalho inicial é de buscar aplicar *machine learning* para detecção de intrusão em redes, o que por si só já é uma tarefa trabalhosa, visto que existem diversas técnicas que podem ser exploradas para manipular os dados e escolher as melhores *features* e formatos delas.

Portanto, a ideia primária é trabalhar de fato com a criação dos modelos, buscando atingir bons resultados por meio das métricas e comparações com outros trabalhos correlatos. Porém, caso o tempo seja viável, pode-se desenvolver algum tipo de aplicação que use um dos modelos, o que à primeira vista parece realmente estar fora dos limites de tempo e esforço.

Referências

[1] "Volume of data information created, captured, copied, and consumed worldwide from 2010 to 2025". Statista, 2022.

[2] BARRETO, Jeanine dos S.; ZANIN, Aline; SARAIVA, Maurício de O. Fundamentos de redes de computadores. Grupo A, 2018. 9788595027138.

[3] OODRICH, Michael T.; TAMASSIA, Roberto. Introdução à Segurança de Computadores. Grupo A, 2012. 9788540701939.
[4] Sultana, N.; Chilamkurti, N.; Peng, W. "Survey on SDN based network intrusion detection system using machine learning approaches".
[5] Ghori K. M.; Abbasi R. A.; Awais M.; (Member, IEEE).; Imran M.; Ullah A.; Szathmary L. "Performance Analysis of Different Types of Machine Learning Classifiers for Non-Technical Loss Detection". IEEE, 2019. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8943419
[6] Ahmad, Z.; Khan, A. S.; Shiang, C. W.; Abdullah, J.; Ahmad F. "Network intrusion detection system: A systematic study of machine learning and deep learning approaches". Wiley, 2020. https://onlinelibrary.wiley.com/doi/10.1002/ett.4150
[7] Alzahrani, A.O.; Alenazi, M.J.F. Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks. Future Internet 2021, 13, 111. https://doi.org/10.3390/fi13050111