Uma proposta de controlador SDN e Aprendizado de Máquina para detecção de ataques por botnets em redes IoT: uma abordagem para o ensino de redes de computadores

Bruno Henrique Graziano Costa[1] **, Antonio Wendell de Oliveira Rodrigues**[2]

[1]Programa de Pós-Graduação em Ciência da Computação - PPGCC
do Instituto Federal do Ceará (IFCE)

bruno.graziano02@aluno.ifce.com.br

[2]PPGCC-IFCE

wendell.rodrigues@ppgcc.ifce.com.br

Abstract. *In the field of computer network education, it is important to use simulated scenarios that resemble real-world environments to enhance learning and knowledge retention. This article describes a proposal for a Software-Defined Networking (SDN) controller that can detect attacks in Internet of Things (IoT) networks. The proposal suggests a high-performance distributed backend with artificial intelligence (AI) using the OpenFlow protocol to quickly intervene in switches connecting sensors and actuators. To validate the proposal, the Bot-IoT dataset and a simulated environment in GNS3 were used. By combining real attack situations and SDN concepts, this provides a suitable environment for understanding the use of artificial intelligence in computer networks.*

Resumo. *No ensino de redes de computadores, o uso de cenários que simulem os ambientes reais é importante para aprendizagem e fixação do conhecimento. Este artigo descreve uma proposta de controlador SDN (Redes Definidas por Software) para detecção de ataques em redes de Internet das Coisas (IoT). Para isso, é proposto um backend distribuído de alto desempenho com IA fazendo uso do protocolo OpenFlow para intervenção imediata nos switches que conectam sensores e atuadores. Para validação da proposta, foi utilizado o dataset Bot-IoT e um ambiente simulado em GNS3. Ao final, unindo situações de ataques reais e conceitos de SDN, tem-se um ambiente propício pra compreensão do uso de inteligência artificial no contexto de redes de computadores.*

1. Introdução

Os ambientes simulados desempenham um papel crucial no ensino de redes de computadores, especialmente no contexto da Internet das Coisas (IoT). Esses ambientes simulam cenários do mundo real e proporcionam uma experiência de aprendizado prática para os alunos. No campo da IoT, onde uma infinidade de dispositivos está interconectada e se comunica entre si, o uso de ambientes simulados torna-se ainda mais importante. Esses ambientes permitem que os alunos explorem as complexidades das redes IoT, compreendam os desafios envolvidos e desenvolvam habilidades em gerenciamento e segurança de redes [Corino et al. 2020]. Este artigo explora a utilização de ambientes simulados para

o ensino de redes de computadores, com um foco específico na IoT, e destaca sua importância em aprimorar a compreensão dos alunos e a aplicação prática dos conceitos de rede nesse campo em constante evolução.

A segurança de redes IoT tem sido uma grande preocupação devido ao crescente número de dispositivos conectados à internet, o que aumenta o risco de ataques de botnets. A utilização de tecnologias como SDN e GNS3 para emular o cenário tem sido uma prática comum para mitigar esses riscos [Li et al. 2019]. Além disso, o uso de SDN controllers com inteligência artificial e machine learning pode ser uma solução eficaz para avaliar os fluxos nos SDN switches e identificar possíveis ameaças de botnets [Kh et al. 2021].

Estudos recentes [Duan et al. 2022] apontam que a utilização de SDN pode fornecer uma camada adicional de segurança para redes IoT, permitindo a criação de políticas de segurança mais flexíveis e escaláveis. Já a utilização de GNS3 permite a criação de ambientes de teste que simulam redes IoT complexas, o que pode ajudar na avaliação e mitigação de riscos de segurança [Yamasaki et al. 2011].

A utilização de SDN *controllers* dotados de inteligência artificial tem se mostrado uma abordagem promissora para a prevenção de ataques de botnets em redes IoT. Um SDN *controller* com machine learning pode identificar fluxos suspeitos e bloquear conexões maliciosas de forma eficiente [Maeda et al. 2019]. Outro estudo realizado em [Costa et al. 2018] propôs um framework de detecção de botnets em redes utilizando técnicas mineração de fluxos e SDN.

Em suma, a utilização de tecnologias como SDN e o emulador GNS3, juntamente com SDN *controllers* dotados de inteligência artificial e machine learning, pode fornecer uma camada adicional de segurança para redes IoT e ajudar na prevenção de ataques de botnets. É importante que as organizações que trabalham com redes IoT estejam cientes dessas tecnologias e as considerem em seus processos de segurança.

2. Revisão Teórica

2.1. Redes Definidas por Software (SDN) e IoT

Redes Definidas por Software (SDN) são um paradigma emergente no campo de redes de computadores, e seu uso tem se mostrado cada vez mais relevante no contexto do ensino de redes e Internet das Coisas (IoT). SDN refere-se a uma abordagem em que o controle e o gerenciamento da rede são separados do hardware subjacente, permitindo uma maior flexibilidade e programabilidade da infraestrutura de rede. No ensino de redes, o uso de SDN proporciona aos alunos a oportunidade de entender e experimentar conceitos avançados de gerenciamento e controle de redes de forma prática. Além disso, no contexto específico da IoT, onde há uma grande diversidade de dispositivos interconectados, a adoção de SDN oferece benefícios significativos, permitindo uma configuração e gerenciamento mais eficientes da rede IoT. Através da combinação de SDN e IoT, os estudantes podem explorar cenários reais e complexos, compreender os desafios de segurança e gerenciamento dessas redes heterogêneas, além de desenvolver habilidades na utilização de soluções baseadas nesta abordagem [Nunez et al. 2023]. Essa integração no ensino de redes permite aos alunos uma compreensão aprofundada do potencial dessa tecnologia inovadora no contexto atual e futuro das redes de computadores. Além disso, o uso

de tecnologias modernas como programação com WebServices pode ser usado de forma automatizada.

2.2. GNS3 (Graphical Network Simulator 3)

O GNS3 é uma plataforma de simulação amplamente utilizada no ensino de redes de computadores e também pode ser aplicado no contexto da Internet das Coisas (IoT). Essa ferramenta oferece um ambiente virtualizado onde os alunos podem criar redes complexas e realizar experimentos práticos sem a necessidade de hardware físico. No ensino de redes de computadores, o uso do GNS3 permite que os alunos experimentem e compreendam os conceitos teóricos aprendidos em sala de aula, implementando topologias de rede, configurando dispositivos e testando protocolos de comunicação [Gil et al. 2014]. Além disso, no contexto específico da IoT, o GNS3 possibilita a simulação de redes de IoT, envolvendo sensores, atuadores e dispositivos inteligentes interconectados. Isso permite que os alunos explorem cenários reais de IoT e compreendam os desafios relacionados à conectividade, segurança e gerenciamento de redes. Ao fornecer uma experiência prática e interativa, o GNS3 contribui para o aprimoramento das habilidades dos alunos no projeto, implementação e solução de problemas. Isso resulta em uma compreensão mais profunda dos conceitos teóricos e um melhor preparo para enfrentar os desafios enfrentados na prática nessas áreas.

3. Metodologia

Para realizar os procedimentos for desenhada uma estrutura de rede conforme a Figura 1.

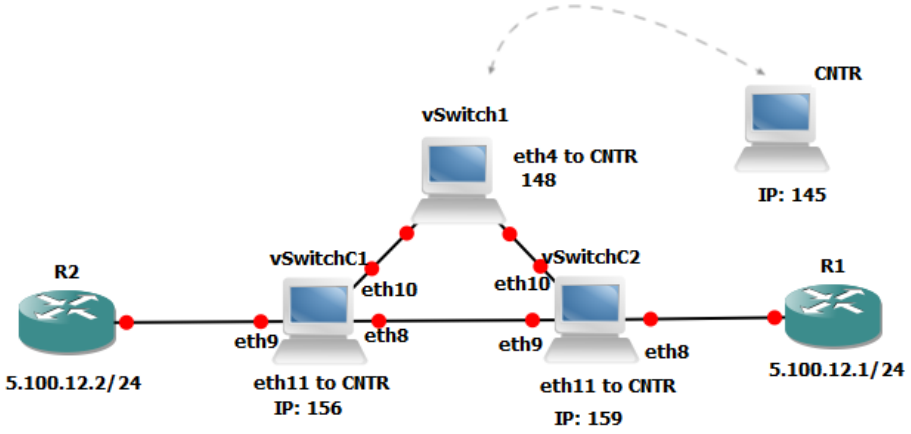

Figura 1. Diagrama Estrutural da Rede de Avaliação. Fonte: autores

A rede é composta por 3 vSwitches (virtual switches) e um controlador SDN centralizado. Os vSwitches são dispositivos que realizam o encaminhamento de pacotes dentro da rede. Cada vSwitch é conectado a dispositivos finais, como computadores ou servidores ou nesta proposta, IoT *devices*, por meio de interfaces virtuais. Os vSwitches, desta forma, desempenham papel importante na forma como os pacotes advindos de redes IoT são encaminhados e analisados por controladores SDN usando ferramentas computacionais de alto nível. O controlador (CNTR) SDN gerencia a lógica de encaminhamento e controle da rede. Ele recebe informações de cada vSwitch sobre o tráfego de pacotes (fluxos) e toma decisões sobre como esses pacotes devem ser encaminhados com base

em políticas pré-definidas. O controlador SDN também pode interagir com os vSwitches para atualizar suas tabelas de encaminhamento. Os vSwitches se comunicam com o controlador por meio do protocolo OpenFlow, que permite que o controlador envie instruções aos vSwitches e receba informações sobre o estado da rede. Dessa forma, o controlador tem uma visão global da rede e pode tomar decisões automatizadas de encaminhamento com base em um plano centralizado.

Com essa configuração básica de rede SDN, é possível implementar políticas de roteamento, como as baseadas em qualidade de serviço (QoS) ou as baseadas em políticas de segurança. O controlador SDN centralizado permite uma maior flexibilidade e adaptabilidade da rede, além de simplificar a configuração e o gerenciamento da rede como um todo.

O procedimento de treinamento para classificação de ataque ou não usando machine learning com o *framework* PyCaret, utilizando os modelos Logistic Regression (lr), K-Nearest Neighbors (knn), Support Vector Machine - Linear Kernel (svm), Naive Bayes (nb) e Decision Tree Classifier (dt), iniciou com a preparação dos dados. O conjunto de dados BotNet-IoT[1] é carregado no *framework* usando uma versão com as 10 características mais importantes do *dataset*. A codificação ou transformação dos atributos categóricos também é feita. Em seguida, o framework é configurado, importando as bibliotecas necessárias e inicializando o ambiente. O treinamento e a avaliação dos modelos são realizados usando a função ***compare_models***, que treina cada modelo usando validação cruzada e fornece uma tabela comparativa com as métricas de desempenho. Com base nessas métricas, o melhor modelo é selecionado. Por fim, o modelo ajustado pode ser utilizado para fazer predições em novos dados, fornecendo classificações de ataque ou não ataque.

4. Resultados Preliminares

A Tabela 1 mostra os resultados obtidos durante fase de treinamento e teste dos modelos. Os modelos lr, dt e nb apresentaram um desempenho geralmente melhor, com altas métricas de desempenho em todas as categorias. No entanto, é importante levar em consideração o tempo de treinamento necessário para cada modelo. O modelo svm teve uma AUC muito baixa, indicando uma baixa capacidade de distinguir as classes. O modelo knn apresentou uma AUC moderada e um tempo de treinamento consideravelmente maior em comparação aos outros modelos. Especificamente para o caso do modelo lr, ele obteve excelente desempenho, com acurácia, recall, precisão e F1-score de 1.0000, indicando uma classificação perfeita das instâncias. Além disso, a área sob a curva ROC (AUC) também foi alta (0.9998), evidenciando uma ótima capacidade de distinguir as classes. O modelo teve um tempo de treinamento de 252.8040 segundos o que viabiliza fases de retreinamento e implementação dentro do processo decisório do controlador SDN. Um ponto estranho observado é o AUC=0 para o svm. Precisa-se de mais análises, mas de antemão é possível supor que houve um erro na configuração dos rótulos do SVM e houve uma classificação invertida. No decorrer do trabalho, isso deve ser melhor diagnosticado e corrigido.

[1] https://research.unsw.edu.au/projects/bot-iot-dataset

Tabela 1. Resultados de desempenho dos modelos

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
lr	1.0000	0.9998	1.0000	1.0000	1.0000	0.9128	0.9150	252.8040
dt	1.0000	0.9611	1.0000	1.0000	1.0000	0.9564	0.9571	66.7510
knn	0.9999	0.8910	1.0000	0.9999	1.0000	0.6593	0.6901	2796.7380
svm	0.9998	0.0000	0.9999	0.9999	0.9999	0.0433	0.0488	67.8410
nb	0.9978	0.9971	0.9979	1.0000	0.9989	0.0776	0.1652	47.0220

5. Conclusões e Perspectivas

Este trabalho encontra-se em andamento e, com base nas avaliações preliminares, já é possível concluir sobre a eficácia do uso de algoritmos de aprendizado de máquina no processo de tomada de decisão para o encaminhamento de pacotes em redes, especificamente na classificação de botnets em redes IoT. Essa aplicação é de grande importância no contexto do ensino de redes, demonstrando o uso de ferramentas modernas para aprimorar a segurança e o desempenho. Ainda há muito trabalho a ser realizado. Como perspectivas para futuros estudos, pretende-se utilizar o simulador *Mininet* para facilitar a implementação pragmática do controlador SDN, empregando o protocolo *OpenFlow*. Além disso, existe o interesse em analisar outros conjuntos de dados disponíveis na literatura para validar diferentes abordagens de classificação.

Referências

Corino, M., Bertagnolli, S., and Schmitt, M. (2020). Desenvolvimento e aplicação de uma estratégia pedagógica para o ensino de redes de computadores com robótica educacional. In *Anais do XXXI Simpósio Brasileiro de Informática na Educação*, pages 1663–1672, Porto Alegre, RS, Brasil. SBC.

Costa, V., Zarpelão, B., Miani, R., and Junior, S. B. (2018). Online detection of botnets on network flows using stream mining. In *Anais do XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 225–238, Porto Alegre, RS, Brasil. SBC.

Duan, L., Zhou, J., Wu, Y., and Xu, W. (2022). A novel and highly efficient botnet detection algorithm based on network traffic analysis of smart systems. *International Journal of Distributed Sensor Networks*, 18(3):15501477211049910.

Gil, P., García, G. J., Delgado, A. D., Medina, R. M., Calderon, A., and Marti, P. (2014). Computer networks virtualization with GNS3: evaluating a solution to optimize resources and achieve a distance learning. In *IEEE Frontiers in Education Conference, FIE 2014, Proceedings, Madrid, Spain, October 22-25, 2014*, pages 1–4. IEEE Computer Society.

Kh, D. R., Botirov, S., and Juraev, F. (2021). A simulation model of a cloud data center based on traditional networks and software-defined network. In *2021 International Conference on Information Science and Communications Technologies (ICISCT)*, pages 1–4. IEEE.

Li, M., Yu, F. R., Si, P., and Zhang, Y. (2019). Energy-efficient machine-to-machine (m2m) communications in virtualized cellular networks with mobile edge computing (mec). *IEEE Transactions on Mobile Computing*, 18(7):1541–1555.

Maeda, S., Kanai, A., Tanimoto, S., Hatashima, T., and Ohkubo, K. (2019). A botnet detection method on sdn using deep learning. In *2019 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–6.

Nunez, A., Ayoka, J., Islam, M. Z., and Ruiz, P. (2023). A brief overview of software-defined networking.

Yamasaki, Y., Miyamoto, Y., Yamato, J., Goto, H., and Sone, H. (2011). Flexible access management system for campus vlan based on openflow. In *Proceedings - 11th IEEE/IPSJ International Symposium on Applications and the Internet, SAINT 2011*, Proceedings - 11th IEEE/IPSJ International Symposium on Applications and the Internet, SAINT 2011, pages 347–351. 11th IEEE/IPSJ International Symposium on Applications and the Internet, SAINT 2011 ; Conference date: 18-07-2011 Through 21-07-2011.