Desafios e Oportunidades na Detecção de Anomalias em SDN Usando Inteligência Computacional

Rivaldo Fernandes[1], **Diego Kreutz**[2], **Ramon Fontes**[1], **Rafael Lopes Gomes**[3], **Roger Immich**[1]

[1] Universidade Federal do Rio Grande do Norte (UFRN)

rivaldofernandes@gmail.com, {ramon.fontes, roger}@imd.ufrn.br

[2]Universidade Federal do Pampa (Unipampa)

diegokreutz@unipampa.edu.br

[3]Universidade Estadual do Ceará (UECE)

rafa.lopes@uece.br

Abstract. *The increasing complexity of computer networks, driven by Software-Defined Networking (SDN), necessitates advanced Computational Intelligence (CI) techniques to enhance security and reliability. In this context, this study conducts a systematic literature mapping on the application of CI for anomaly detection in SDN. The analysis highlights various techniques and architectures, emphasizing the importance of diverse datasets—including real-world networks—to ensure model generalization. Key challenges such as high computational costs, the security of CI modules, and model interpretability are discussed. Finally, the study underscores emerging opportunities and the need for flexible architectures that integrate multiple CI techniques to improve anomaly detection in SDN.*

Resumo. *A complexidade crescente das redes de computadores, impulsionada pelas Redes Definidas por Software (SDN), exige técnicas avançadas de Inteligência Computacional (IC) para melhorar segurança e confiabilidade. Neste contexto, este trabalho realiza um mapeamento sistemático da literatura sobre o uso da IC na detecção de anomalias em SDN. A análise revela diversas técnicas e arquiteturas, além da importância de datasets variados, incluindo redes reais, para garantir a generalização dos modelos. São discutidos desafios como alto custo computacional, segurança dos módulos de IC e interpretabilidade dos modelos. Por fim, o estudo destaca oportunidades e a necessidade de arquiteturas flexíveis que integrem diferentes técnicas de IC para aprimorar a detecção de anomalias em SDN.*

1. Introdução

As Redes Definidas por Software (SDN) oferecem flexibilidade e controle programático, mas sua crescente complexidade e centralização do controle geram novos desafios de segurança, tornando a detecção de anomalias uma área de pesquisa crucial [do Prado et al. 2021, Bittencourt et al. 2018]. Neste cenário, a inteligência computacional (IC) possibilita a análise de grandes volumes de dados de rede e a identificação de padrões anormais que indicam ataques, falhas ou comportamentos suspeitos.

Neste sentido, questões de autenticação e troca segura de chaves são de grande importância para garantir a integridade das comunicações em ambientes SDN [Silva et al. 2023]. Complementarmente, a implementação de criptografia e troca de chaves diretamente no plano de dados programável pode reforçar a segurança [Oliveira et al. 2021], aspecto essencial para garantir a confiabilidade do tráfego analisado por mecanismos de detecção de anomalias baseados em IC.

Este trabalho apresenta uma revisão sistemática da literatura sobre a aplicação de IC para detecção de anomalias em SDN, com o objetivo de mapear o estado da arte da pesquisa, identificando as principais técnicas, arquiteturas, datasets, desafios e oportunidades. A análise revela uma diversidade de algoritmos de IC, incluindo aprendizado supervisionado, não supervisionado, profundo e por reforço.

A pesquisa identificou desafios como a necessidade de alto poder computacional, a segurança contra ataques de envenenamento, a interpretabilidade dos modelos e a vulnerabilidade do controlador SDN como ponto único de falha.

Este trabalho contribui para o avanço da pesquisa em detecção de anomalias em SDN ao: (1) fornecer um panorama das técnicas, arquiteturas e datasets utilizados; (2) identificar os desafios e oportunidades para pesquisas futuras; e (3) estabelecer as bases para o desenvolvimento de arquiteturas flexíveis e adaptáveis que integrem diferentes técnicas de IC.

O restante deste trabalho está estruturado da seguinte forma. A Seção 2 descreve a metodologia do mapeamento sistemático, e a visão geral dos resultados estão na Seção 3. A Seção 4 discute os trabalhos relacionados à detecção de anomalias em SDN, com ênfase nas arquiteturas, algoritmos, datasets, desafios e oportunidades. A Seção 5 apresenta as considerações finais.

2. Metodologia do mapeamento sistemático

O mapeamento sistemático foi baseado nas regras propostas por [Petersen et al. 2008]. Os passos do mapeamento sistemático da literatura estão documentados nas seções subsequentes.

2.1. Perguntas da Pesquisa

Considerando o escopo desta revisão as perguntas da pesquisa foram:

PP1 - Quais são as principais características das arquiteturas e *frameworks* utilizados nos sistemas para detecção de anomalias em SDN?
PP2 - Quais são os padrões e algoritmos de aprendizado de máquina utilizados para detecção de anomalias em redes?
PP3 - Quais os desafios e oportunidades para detecção de anomalias em SDN?

Na PP1 a intenção foi analisar os requisitos funcionais e não funcionais utilizados por arquiteturas e *frameworks* definidos nos estudos analisados. Já na PP2 a intenção foi mapear os principais algoritmos e padrões de inteligência computacional que estão sendo utilizados nos estudos da área. Enquanto na PP3 foi detalhar os desafios e oportunidades que estes estudos encontraram.

2.2. Processo de busca

A seleção dos estudos foi feita no Scopus da Elsevier[1]. A Scopus destaca-se como uma base de dados de referência nessas áreas, indexando periódicos de alto impacto e conferências de renome internacional. Assim, a *string* de busca definida foi: ("*software defined network*" OU "sdn" OU "*software-defined network*") E ("*artificial intelligence*") E ("*anomaly*").

[1]http://scopus.com

2.3. Critério de inclusão e exclusão

Os critérios de inclusão utilizados são descritos abaixo.

CI1 - Trabalho publicado e disponível por completo em formato digital nas bases de dados científicas.
CI2 - Artigo baseado em pesquisa científica.
CI3 - Que apresente informações sobre a arquitetura sistêmica utilizada e ou os *frameworks* utilizados.
CI4 - Que contenha informações sobre quais foram os algoritmos ou os padrões de inteligência computacional utilizados.

Os critérios de exclusão aplicados foram:

CE1 - Não apresenta proposta de implementação ou desenvolvimento utilizando SDN.
CE2 - Não identifica os algoritmos/técnicas utilizados.
CE3 - Não identifica os componentes de arquitetura utilizados para armazenamento e processamento de dados ou para treinamento dos algoritmos.
CE4 - Artigos curtos (3 páginas ou menos).

Os critérios de inclusão e exclusão adotados, baseados em [Dybå and Dingsøyr 2008], consideram três aspectos essenciais para a avaliação de estudos de revisão de literatura: rigor, credibilidade e relevância. O rigor analisa se os principais métodos de pesquisa foram aplicados de maneira completa e apropriada; a credibilidade avalia se os resultados são bem apresentados e significativos; e a relevância investiga a utilidade das descobertas para a indústria de software e hardware, bem como para a comunidade de pesquisa.

3. Visão geral da revisão sistemática

A Figura 1 apresenta as etapas do processo de seleção dos estudos. No primeiro passo, esta busca retornou 696 estudos quando foi pesquisada sem o termo para anomalia, em seguida, se adicionou o termo anomalia e a busca foi refeita, desta vez retornou 37 estudos no passo 2. Após a aplicação dos critérios de inclusão e exclusão, restaram 26 estudos. Estes foram utilizados para responderem às questões de pesquisa propostas.

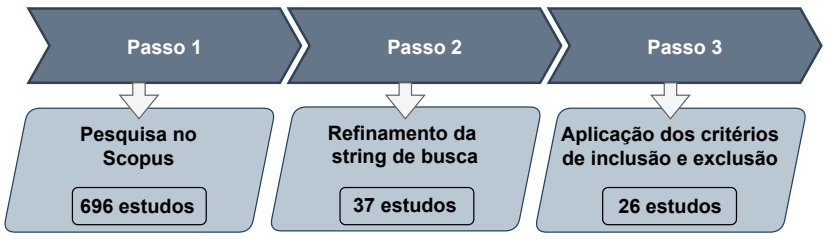

Figura 1. Passo a passo do processo de seleção dos estudos

A Figura 2 apresenta a distribuição de estudos por ano. São apresentados os valores antes e depois dos critérios de inclusão e exclusão. Um dos grandes desafios para este tipo de estudo é obter dados de tráfego de redes reais para treinar os modelos de inteligência computacional. A Figura 3 apresenta a utilização dos *datasets* em função do ano.

É importante ressaltar que alguns trabalhos utilizam mais de um *datasets*. Ainda é possível perceber que não foram utilizados *datasets* em 2016, 2019 e 2022. Até o ano 2020 a principal fonte de dados utilizada por pesquisas era a fonte chamada KDD, a partir de 2021 outras fontes de dados começaram a ser utilizadas, normalmente estas fontes são mais especializadas como fonte de tráfego de dados de redes IoT, *Backbone*

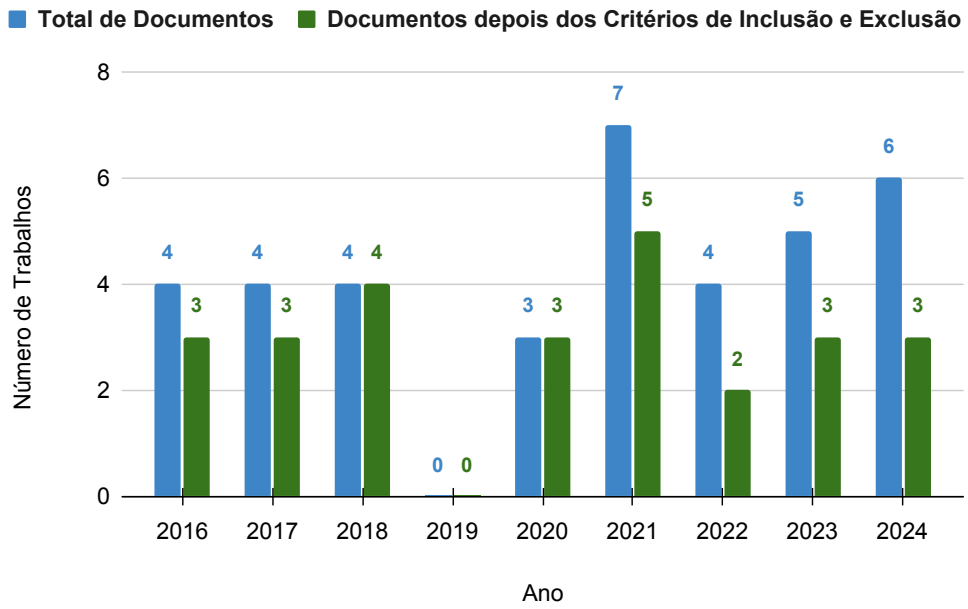

Figura 2. Distribuição de estudos por ano

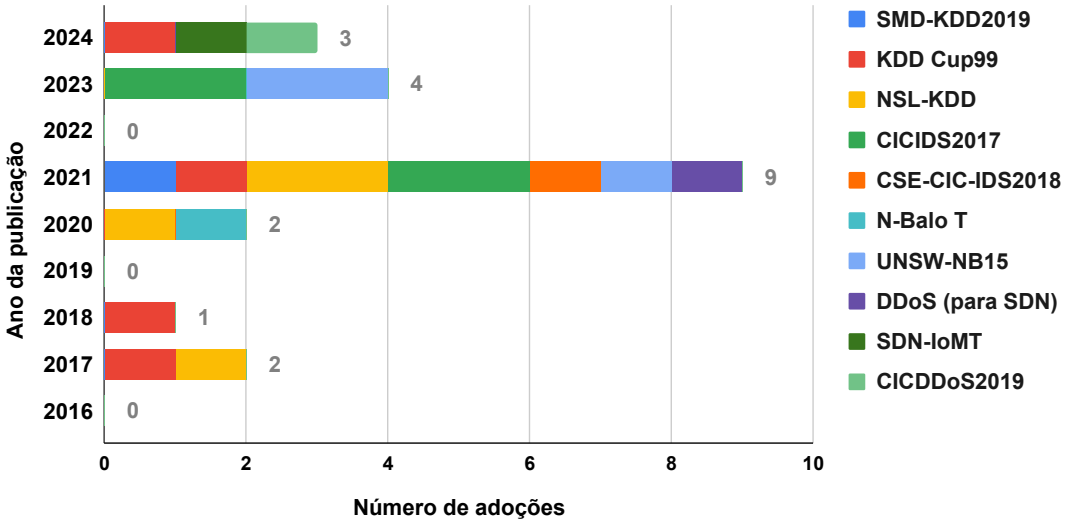

Figura 3. Origem da Fonte de dados utilizada por cada ano

ou contendo informações específicas a um tipo de ataque como o de Negação de Serviço Distribuído. Adicionalmente, apenas quatro pesquisas utilizaram mais de uma fonte de dados e algumas adicionalmente também geraram dados em redes próprias.

Em relação as fontes de dados, destacamos que o estudo [Krzemien et al. 2021] utilizou 6 fontes de dados distintas e os trabalhos [Al-Ameer et al. 2023, Abd Al-Ameer and Bhaya 2023, Das et al. 2021] utilizaram duas fontes de dados distintas. Os demais estudos, [Min et al. 2024, Zabeehullah et al. 2024, Protogerou and et. al. 2022, Le et al. 2021, Dinh and Park 2021, Bagaa et al. 2020, Tsogbaatar et al. 2020, Starke et al. 2018, Abubakar and Pranggono 2017, Song et al. 2017], utilizaram somente uma fonte de dados. Os demais trabalhos não especificaram.

Adicionalmente, foi possível identificar 12 estudos criaram suas próprias redes virtuais para utilizar métricas geradas pelo tráfego de dados nestas redes, os estudos em questão foram os [Pan et al. 2022, Tsogbaatar et al. 2020, Mathas et al. 2018, Starke et al. 2018, Abubakar and Pranggono 2017, Song et al. 2017, Jagadeesan and Mendiratta 2016, Nobakht et al. 2016, Santos da Silva et al. 2016, Le et al. 2021, Qi et al. 2021, Phan et al. 2020]. Apenas 6 pesquisas não utilizaram redes virtuais: [Boero et al. 2017, Protogerou and et. al. 2022, Krzemien et al. 2021, Das et al. 2021, Dinh and Park 2021, Bagaa et al. 2020]. E duas não informaram, [Zhao et al. 2018, Dawoud et al. 2018]. Entre estes, apenas 4 estudos, [Pan et al. 2022, Tsogbaatar et al. 2020, Boero et al. 2017, Nobakht et al. 2016], criaram uma rede física tradicional com equipamentos de rede físicos para coletar as informações necessárias para treinar seus módulos de aprendizagem de máquina para detecção de anomalias.

É possível destacar que das 13 pesquisas que criaram redes virtuais, 9 utilizaram Mininet e 5 o *Open vSwitch* (OVS) para criar suas redes virtuais. O controlador SDN *Open Network Operating System* (ONOS) foi o mais utilizado com 10 pesquisas, em seguida vem o *OpenDaylight* e o *Floodlight* com 4 pesquisas cada.

Também foram analisadas as plataformas de dados que foram utilizadas. A Figura 4 apresenta a lista das plataformas de dados utilizadas com a quantidade de estudos que utilizou cada plataforma. Ao total 14 estudos não informaram qual e nem se utilizaram plataforma de dados, são eles [Al-Ameer et al. 2023, Abd Al-Ameer and Bhaya 2023, AĞCA et al. 2023, Pan et al. 2022, Tsogbaatar et al. 2020, Zhao et al. 2018, Abubakar and Pranggono 2017, Boero et al. 2017, Song et al. 2017, Nobakht et al. 2016, Santos da Silva et al. 2016, Le et al. 2021, Qi et al. 2021, Phan et al. 2020].

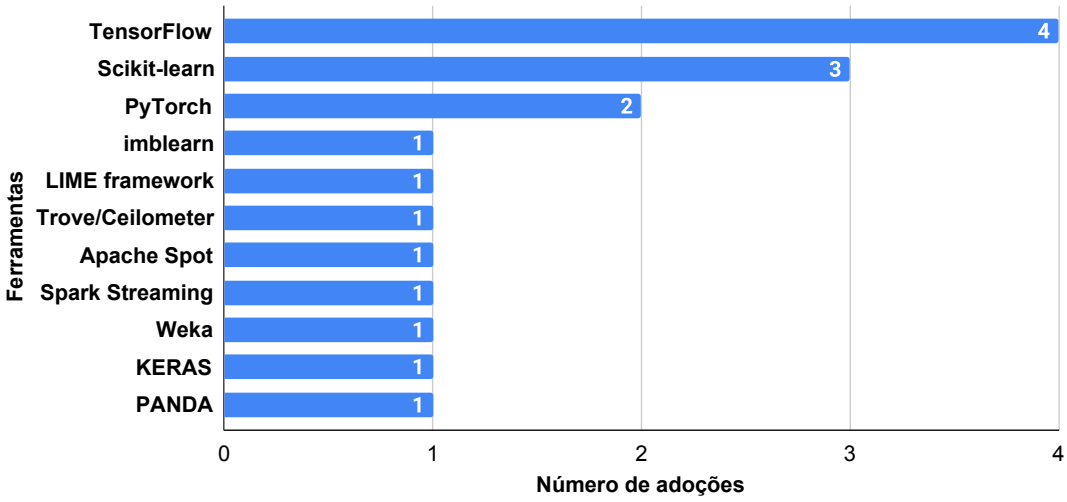

Figura 4. Quantidade de vezes que cada plataforma de dados foi utilizada

4. Detecção de Anomalias em SDN com IC

4.1. Quais são as principais características das arquiteturas utilizadas nos sistemas e *frameworks* para detecção de anomalias em SDN?

O estudo de [Pan et al. 2022] propôs uma arquitetura para coleta de dados por agentes na borda da *layer* de pacotes sobre a *layer* óptica. Os dados são analisados pelo componente

de IC, que envia ações corretivas ao controlador SDN. Em [Protogerou and et. al. 2022], foi definida uma arquitetura de *ciber*segurança para IoT, composta por quatro componentes interconectados e um sistema de detecção de ameaças e anomalias baseado em IA. A proposta de [Qi et al. 2021] coletou periodicamente Indicadores de Performance Chave (*Key Performance Indicator* - KPI) e aplicou algoritmos de detecção de anomalias, permitindo ao controlador SDN monitorar detalhadamente dispositivos e links da rede. Já [Phan et al. 2020] focou na melhoria da detecção de *cyberattacks* em SDN por meio de um mecanismo de monitoramento detalhado do tráfego.

O *framework* de [Bagaa et al. 2020], baseado em aprendizado de máquina, amplia automaticamente a segurança no domínio IoT, utilizando SDN e Virtualização de Funções de Rede (*Network Function Virtualization* - NFV) para mitigar ameaças. Em [Tsogbaatar et al. 2020], o *framework* inclui módulos para coleta e processamento, aprendizado de máquina, detecção de tráfego malicioso, gerenciamento de fluxo de dados e manutenção de tabelas de estado e regras de encaminhamento. O estudo de [Zhao et al. 2018] propõe uma arquitetura para SDN em redes ópticas, baseada em Redes Ópticas Definidas por *Software* (*Software-Defined Optical Network* - SDON), permitindo o controle de múltiplos recursos ópticos. Já [Starke et al. 2018] apresenta um modelo onde vários controladores SDN compartilham topologia e estado da rede em um sistema distribuído, mantendo o controle centralizado da SDN.

O artigo [AĞCA et al. 2023] introduz a metodologia Trusted Distributed AI (TDAI), que cria um ambiente confiável orientado por software para maximizar a cooperação entre tarefas e reduzir erros em sistemas de IA distribuídos. Em [Alshammari et al. 2024], um mecanismo de detecção de anomalias para NFV MANO combina monitoramento adaptativo e funções de segurança para melhorar a experiência do usuário. A proposta de [Zabeehullah et al. 2024] apresenta uma estrutura baseada em SDN e aprendizado profundo para detectar anomalias e ataques em redes de IoT Médico (IoMT) com grandes volumes de dados desequilibrados. Já [Al-Ameer et al. 2023] propõe um sistema inteligente de detecção de intrusão em SDN, baseado em aprendizado federado multimodelo, preservando a privacidade dos dados.

O artigo [Min et al. 2024] propõe a estrutura Cu-BLSTMGRU, uma solução de detecção de intrusões baseada em IA e orquestrada por SDN, voltada para redes industriais de IoT (IIoT) com recursos limitados, combinando BLSTM e GRU. Por fim, [Abd Al-Ameer and Bhaya 2023] apresenta uma abordagem de detecção de anomalias em SDN que integra Aprendizado Federado (FL) e LSTM, permitindo que switches SDN treinem colaborativamente um modelo universal sem comprometer a privacidade dos dados.

As arquiteturas analisadas apresentam similaridades apenas no nível de camadas, geralmente organizadas em três: uma para a rede e seus dispositivos, outra para análise de dados e treinamento de modelos de IC, e uma para softwares que interagem com a rede. No entanto, dentro de cada camada, não há padrões amplamente adotados.

4.2. Quais são os padrões e algoritmos de aprendizado de máquina utilizados para detecção de anomalias em redes?

O algoritmo de [Protogerou and et. al. 2022], baseado em GNN, foca em ataques DoS, mas também detectou varredura de porta e inundação de UDP com maior precisão que SVM, DT e RF. Em [Qi et al. 2021], os autores utilizam uma rede convolucional baseada em grafos para detecção de anomalias, empregando *Group Anomaly Detection* (GAD). O estudo [Krzemien et al. 2021] testou seis conjuntos de dados com validação cruzada e os algoritmos RF, *XGBoost* e redes neurais, obtendo precisão entre 88,49% e 99,28%. Foram utilizadas bibliotecas como *scikit-learn* e TensorFlow. Já [Das et al. 2021] propõe

uma arquitetura com classificadores de IC para aumentar a confiabilidade das previsões, utilizando Inteligência Artificial Explicável (*Explainable Artificial Intelligence* - XAI) para interpretar os principais recursos associados às anomalias detectadas.

Os resultados de [Bagaa et al. 2020] mostram que RF teve bom desempenho geral, mas baixa precisão para ataques R2L e U2R. O J48 apresentou boa detecção com baixa taxa de erro, mas também teve desempenho insatisfatório em ataques U2R. Em [Mathas et al. 2018], *Latent Dirichlet Allocation* (LDA) foi usado para detectar padrões de anomalias no tráfego, diferenciando-se dos classificadores tradicionais por ser um algoritmo de Processamento de Linguagem Natural (*Natural Language Processing* - NLP). O experimento de [Nobakht et al. 2016] avaliou o *framework* IoT-IDM com classificação de regressão logística. O modelo linear detectou acessos não autorizados com 94,25% de precisão e 85,05% de revocação, enquanto o modelo não linear atingiu 98,53% e 95,94%, respectivamente.

O estudo [Abubakar and Pranggono 2017] indica que o Reconhecimento de Padrão teve melhor desempenho na detecção de anomalias, com 97,3% de taxa de acerto. Inicialmente, a curva de ajuste apresentou 89,5% de precisão, mas a reconfiguração dos pesos aprimorou os resultados. Em contrapartida, a Rede Neural de Série Temporal teve pior desempenho, com alto tempo de treinamento e retreinamento difícil.

A precisão da detecção de anomalias varia conforme o algoritmo implementado e o conjunto de dados utilizado. No entanto, nenhum estudo analisou a variação da precisão entre diferentes *datasets* para os mesmos tipos de anomalias, o que poderia indicar a adequação de determinados algoritmos a diferentes redes. Destaca-se também o uso do XAI para aprimorar a interpretabilidade dos modelos de IC, uma limitação recorrente nos trabalhos analisados.

4.3. Quais os desafios e oportunidades para detecção de anomalias em SDN utilizando aprendizado de máquina?

A Figura 5 apresenta os principais desafios e oportunidades identificados nos estudos analisados. O trabalho [Pan et al. 2022] destaca que, embora a automação de redes seja promissora, a redução da intervenção humana exige cautela quanto à segurança. Modelos de IC usados para automação podem ser comprometidos por ataques de envenenamento de dados, nos quais agentes mal-intencionados manipulam amostras adversariais para enganar o sistema. O estudo [Protogerou and et. al. 2022] demonstra que soluções baseadas em IA oferecem melhor desempenho em comparação com métodos tradicionais, lidando com desafios de redes IoT de grande escala, que exigem baixa latência e eficiência de recursos. Além disso, os modelos de IA podem aprender a mitigar novos ataques.

Já o trabalho de [Qi et al. 2021] aponta que, diferentemente de áreas como visão computacional e NLP, a rede enfrenta cenários diversos sem padrões universais para definir a verdade absoluta. Isso, aliado ao ruído nos dados, dificulta a rotulagem precisa, tornando modelos não supervisionados e semissupervisionados mais adequados. AIOps precisa levar em conta a lógica interna dos serviços e as características dos dados para projetar algoritmos eficazes.

Os trabalhos [Qi et al. 2021] e [Das et al. 2021] ressaltam a falta de explicabilidade nos sistemas baseados em IC, muitas vezes tratados como "caixas-pretas". Isso dificulta a identificação das causas das anomalias. Para mitigar esse problema, propuseram o CEAD, um pipeline de IA que melhora a confiabilidade da detecção de anomalias em SDN, apresentando melhor desempenho que SVM e MLP e resultados comparáveis ao RF.

O estudo de [Dinh and Park 2021] aborda ataques de Negação Econômica de Sus-

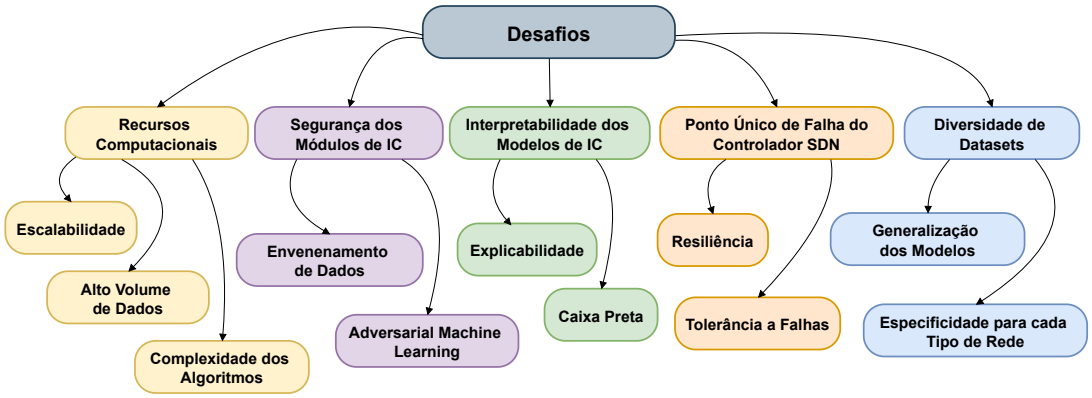

Figura 5. Desafios na detecção de anomalias em SDN

tentabilidade (EDoS), que exploram mecanismos de cobrança pré-paga em serviços de nuvem, forçando clientes a custos extras. Os autores propõem um sistema para mitigar esses ataques, dada a escassez de soluções eficazes. Em [Bagaa et al. 2020] é enfatizado que, com a evolução da IoT, sistemas de IA precisarão se reconfigurar autonomamente para lidar com ataques desconhecidos. Além disso, a segurança exige recursos adicionais, podendo impactar o desempenho, tornando necessário equilibrar segurança e qualidade do serviço.

Em [Mathas et al. 2018] são investigadas vulnerabilidades de algoritmos de IA a ataques de envenenamento, que comprometem modelos e resultam em erros de classificação, como falsos positivos e negativos. O estudo de [Dawoud et al. 2018] analisa a segurança no SDN e destacam que o protocolo *OpenFlow* é suscetível a ataques, como DoS em tabelas de fluxo e canais de controle. Sem criptografia adequada, a comunicação entre controlador e dispositivos fica vulnerável a ataques intermediários, comprometendo a estabilidade da rede.

O estudo [Song et al. 2017] identifica desafios como alta dimensionalidade e tamanho da amostra, que dificultam a escalabilidade, armazenamento e precisão dos modelos. Além disso, o roteamento incorreto de tráfego malicioso pode comprometer a confiabilidade do SDN e facilitar ataques DoS. Adicionalmente, em [Starke et al. 2018] são destacadas a vulnerabilidade de um ponto único de falha no controlador centralizado do SDN. Para redes ciber-físicas em grande escala, novas abordagens devem garantir resiliência sem comprometer a visão global do SDN.

Os desafios identificados mostram a necessidade de aprimorar a detecção de anomalias causadas por amostras adversariais que manipulam dados para enganar os modelos de IC. Além disso, a falta de explicabilidade dificulta a escolha das características mais adequadas para treinamento e monitoramento. Por fim, a alta dimensionalidade dos dados impõe desafios computacionais e estatísticos à execução e ao treinamento dos modelos de IC.

5. Considerações finais

Os principais desafios identificados neste mapeamento incluem a alta demanda computacional para o treinamento e execução de modelos de IC, a vulnerabilidade ao ponto único de falha nas arquiteturas SDN, a falta de interpretabilidade dos modelos, a confiança limitada na segurança desses módulos para automação total da rede e a ausência de uma arquitetura de referência que integre aprendizado de máquina para detecção de anomalias. Além disso, não há consenso sobre as melhores técnicas para essa área, e nenhum estudo

analisou a variação na precisão da detecção entre diferentes *datasets* para o mesmo tipo de anomalia. Essa análise poderia indicar que certos algoritmos são mais eficazes em contextos específicos, ressaltando a necessidade de arquiteturas flexíveis, capazes de integrar e adaptar diferentes técnicas de IA. Por fim, a inexistência de uma arquitetura de referência padronizada revela uma lacuna na área. Isso abre espaço para pesquisas que desenvolvam modelos capazes de suportar diferentes algoritmos de IC em distintos cenários de detecção de anomalias em SDN.

Referências

Abd Al-Ameer, A. A. and Bhaya, W. S. (2023). Enhanced intrusion detection in software-defined networks through federated learning and deep learning. *Ingenierie des Systemes d'Information*, 28(5):1213.

Abubakar, A. and Pranggono, B. (2017). Machine learning based intrusion detection system for software defined networks. In *2017 seventh international conference on emerging security technologies (EST)*, pages 138–143. IEEE, IEEE.

Al-Ameer, A., Asraa, A., and Bhaya, W. S. (2023). Intelligent intrusion detection based on multi-model federated learning for software defined network. *International Journal of Safety & Security Engineering*, 13(6).

Alshammari, N. et al. (2024). Security monitoring and management for the network services in the orchestration of sdn-nfv environment using machine learning techniques. *Computer Systems Science and Engineering*, 48(2):363–394.

AĞCA, M. A., Faye, S., and Khadraoui, D. (2023). Trusted distributed artificial intelligence (tdai). *IEEE Access*, 11:113307–113323.

Bagaa, M., Taleb, T., Bernabe, J. B., and Skarmeta, A. (2020). A machine learning security framework for iot systems. *IEEE Access*, 8:114066–114077.

Bittencourt, L., Immich, R., Sakellariou, R., Fonseca, N., Madeira, E., Curado, M., Villas, L., DaSilva, L., Lee, C., and Rana, O. (2018). The internet of things, fog and cloud continuum: Integration and challenges. *Internet of Things*, 3-4:134 – 155.

Boero, L., Marchese, M., and Zappatore, S. (2017). Support vector machine meets software defined networking in ids domain. In *Inter. Teletraffic Congress (ITC)*. IEEE.

Das, T., Shukla, R., and Sengupta, S. (2021). The devil is in the details: Confident & explainable anomaly detector for software-defined networks. pages 1–5.

Dawoud, A. A., Shahristani, S. S., and Raun, C. (2018). A deep learning framework to enhance software defined networks security. In *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. IEEE.

Dinh, P. T. and Park, M. (2021). R-edos: Robust economic denial of sustainability detection in an sdn-based cloud through stochastic recurrent neural network. *IEEE Access*.

do Prado, P. F., Peixoto, M. L. M., Araújo, M. C., Gama, E. S., Gonçalves, D. M., Silva, M. V. S., Immich, R., Madeira, E. R. M., and Bittencourt, L. F. (2021). *Mobile Edge Computing for Content Distribution and Mobility Support in Smart Cities*, pages 473–500. Springer International Publishing, Cham.

Dybå, T. and Dingsøyr, T. (2008). Empirical studies of agile software development: A systematic review. *Information and Software Technology*, 50(9-10):833–859.

Jagadeesan, L. J. and Mendiratta, V. (2016). Programming the network: Application software faults in software-defined networks. In *2016 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, pages 125–131. IEEE.

Krzemien, W., Jedrasiak, K., Nawrat, A., and Daniec, K. (2021). Anomaly detection in software-defined networks using cross-validation. In *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pages 1–7. IEEE.

Le, D.-H., Tran, H.-A., Souihi, S., and Mellouk, A. (2021). An ai-based traffic matrix prediction solution for software-defined network. In *ICC 2021 - IEEE International Conference on Communications*, pages 1–6. IEEE.

Mathas, C. M., Segou, O. E., Xylouris, G., Christinakis, D., Kourtis, M.-A., Vassilakis, C., and Kourtis, A. (2018). Evaluation of apache spot's machine learning capabilities in an sdn/nfv enabled environment. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018.

Min, W., Almughalles, W., Muthanna, M. S. A., Ouamri, M. A., Muthanna, A., Hong, S., and Abd El-Latif, A. A. (2024). An sdn-orchestrated artificial intelligence-empowered framework to combat intrusions in the next generation cyber-physical systems. *HUMAN-CENTRIC COMPUTING AND INFORMATION SCIENCES*, 14.

Nobakht, M., Sivaraman, V., and Boreli, R. (2016). A host-based intrusion detection and mitigation framework for smart home iot using openflow. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pages 147–156. IEEE.

Oliveira, I., Neto, E., Immich, R., Fontes, R., Neto, A., Rodriguez, F., and Rothenberg, C. E. (2021). dh-aes-p4: On-premise encryption and in-band key-exchange in p4 fully programmable data planes. In *2021 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pages 148–153.

Pan, X., Yang, H., Xu, Z., and Zhu, Z. (2022). Adversarial analysis of ml-based anomaly detection in multi-layer network automation. In *Journal of Lightwave Technology*, volume 40, pages 4934–4944. IEEE.

Petersen, K., Feldt, R., Mujtaba, S., and Mattsson, M. (2008). Systematic mapping studies in software engineering. In *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering*, EASE'08.

Phan, T. V., Nguyen, T. G., Dao, N.-N., Huong, T. T., Thanh, N. H., and Bauschert, T. (2020). Deepguard: Efficient anomaly detection in sdn with fine-grained traffic flow monitoring. *IEEE Transactions on Network and Service Management*, 17(3).

Protogerou, A. and et. al. (2022). Time series network data enabling distributed intelligence. a holistic iot security platform solution. In *Electronics*. MDPI.

Qi, Q., Shen, R., Wang, J., Sun, H., Guo, S., and Liao, J. (2021). Spatial-temporal learning-based artificial intelligence for it operations in the edge network. In *IEEE Network*, volume 35, pages 197–203. IEEE.

Santos da Silva, A., Wickboldt, J. A., Granville, L. Z., and Schaeffer-Filho, A. (2016). Atlantic: A framework for anomaly traffic detection, classification, and mitigation in sdn. In *2016 IEEE/IFIP Network Operations and Management Symposium*. IEEE.

Silva, D., Fontes, R., Neto, A., Silva, G., and Immich, R. (2023). Esquema de autenticação e acordo de chaves para internet das coisas. In *Anais do XXVIII Workshop de Gerência e Operação de Redes e Serviços*, pages 125–138, Porto Alegre, RS, Brasil. SBC.

Song, C., Park, Y., Golani, K., Kim, Y., Bhatt, K., and Goswami, K. (2017). Machine-learning based threat-aware system in software defined networks. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)*. IEEE.

Starke, A., McNair, J., Trevizan, R., Bretas, A., Peeples, J., and Zare, A. (2018). Toward resilient smart grid communications using distributed sdn with ml-based anomaly detection. In *Wired/Wireless Internet Communications*.

Tsogbaatar, E., Bhuyan, M. H., Taenaka, Y., Fall, D., Gonchigsumlaa, K., Elmroth, E., and Kadobayashi, Y. (2020). *SDN-Enabled IoT Anomaly Detection Using Ensemble Learning*. IFIP Advances in Information and Communication Technology. Springer.

Zabeehullah, Arif, F., Khan, N. A., Haq, Q. M. u., Asim, M., and Ahmad, S. (2024). An sdn-ai-based approach for detecting anomalies in imbalance data within a network of smart medical devices. *IEEE Consumer Electronics Magazine*, 13(6):28–36.

Zhao, Y., Yan, B., Liu, D., He, Y., Wang, D., and Zhang, J. (2018). Soon: self-optimizing optical networks with machine learning. *Opt. Express*, 26(22):28713–28726.