Estado da arte sobre ferramentas de análise de tráfego anômalo em sistemas críticos

Ronys Wellington Rodrigues de Santana[1] (IC), Otávio de S. M. Gomes (PQ)[1]
[1]*Universidade Federal de Itajubá (UNIFEI).*

Palavras-chave: Cibersegurança, Detecção de Anomalias, Redes de Comunicação, Infraestruturas Críticas, Aprendizado de Máquina.

Introdução

A cibersegurança é essencial para a defesa de dados sensíveis de empresas, das forças armadas e de países, sendo fundamental para as estratégias de defesa no ciberespaço. Conforme destacado por Cujabante Villamil et al. (2020), a soberania e a segurança nacionais dependem de uma ciberdefesa eficaz, que se adapta continuamente às novas ameaças. Um cenário em que a falta de investimento em cibersegurança coloca em risco as infraestruturas críticas e a integridade de dados corporativos e governamentais é evidente. O país enfrenta desafios significativos devido a um cenário de ameaças que evolui rapidamente, onde a ocorrência de ataques cibernéticos não é uma possibilidade, mas uma inevitabilidade (PIETERSE, 2021).

O impacto global da pandemia de COVID-19 acelerou a necessidade de fortalecer as medidas de cibersegurança, como indicado por Chigada e Madzinga (2021). Essa situação não apenas ampliou as oportunidades para ataques cibernéticos, visando principalmente setores como serviços financeiros, saúde e departamentos governamentais, mas também destacou a necessidade urgente de um paradigma proativo na implementação de protocolos de cibersegurança.

Este artigo visa realizar um levantamento do estado da arte sobre a análise de tráfego anômalo em sistemas críticos, além de uma revisão sistemática dos artigos selecionados nesta busca. O objetivo é identificar os principais autores, trabalhos mais influentes e as tendências emergentes no campo da cibersegurança em redes de comunicação, particularmente em relação à detecção e mitigação de ameaças cibernéticas em redes de sistemas críticos.

1. Desenvolvimento e Desafios dos Sistemas de Detecção de Intrusão

Com o aumento no volume de dados de rede e a distribuição dessas informações na nuvem, os sistemas tradicionais de detecção de intrusão enfrentam limitações de capacidade de processamento. As taxas de detecção acima de 94% e a baixa taxa de falsos positivos reforçam a viabilidade desses sistemas mais robustos e baseados em nuvem (YOU; WANG, 2022). Técnicas como o uso de autoencoders e deep learning também têm mostrado eficácia na detecção de anomalias e intrusões, permitindo uma análise mais precisa (ORTEGA-FERNANDEZ et al., 2023).

2. Impacto da Inteligência Artificial e Aprendizado de Máquina

A adoção de técnicas avançadas de inteligência artificial, especialmente redes neurais convolucionais (ConvNet), tem sido uma ferramenta crucial para a análise e detecção de ameaças. A transferência de conhecimento para melhorar a detecção de intrusões demonstra melhorias significativas em precisão nos conjuntos de dados NSL-KDD. Além disso, a utilização de técnicas de inteligência artificial na análise de intrusões tem sido um dos assuntos frequentemente pesquisados nos últimos cinco anos (WU et al., 2019).

Estudos sobre perturbações adversariais mostram que os sistemas de aprendizado de máquina podem ser vulneráveis a ataques que manipulam suas entradas. Assim, aumenta-se a importância da segurança e privacidade no aprendizado de máquina, enfatizando a necessidade de desenvolver modelos robustos contra essas técnicas de ataque (PAPERNOT et al., 2018).

Metodologia

A metodologia deste estudo foi baseada em um estudo do estado da arte focada nas ferramentas de detecção de anomalias em sistemas críticos.

A primeira etapa da análise utilizou as seguintes palavras-chave na plataforma Web of Science: “Nozomi Cybersecurity,” “network traffic analysis,”

"Cybersecurity," "Cybersecurity Wireshark," "network intrusion detection," e "telecommunication traffic Cybersecurity." Esta busca inicial resultou em 3.812 artigos, que foram então processados e analisados através da ferramenta VOSviewer para identificação de palavras-chave relevantes.

Com base nessa análise, foram selecionadas novas palavras-chave que compuseram a pesquisa subsequente, resultando nas strings de busca:

- "network traffic analysis Cybersecurity critical systems"
- "Cybersecurity Wireshark"
- "network intrusion detection critical systems"
- "telecommunication traffic Cybersecurity critical systems"

Essa busca refinada resultou em 110 artigos.

Critérios de Inclusão: Foram incluídas palavras-chave bem avaliadas pela análise no VOSviewer, que estivessem em alinhamento direto com o tema proposto.
Critérios de Exclusão: Foram excluídas palavras de caráter genérico para evitar um aumento excessivo no número de artigos e palavras ambíguas que poderiam remeter a temas diversos, como medicina, que frequentemente se sobrepõem terminologicamente com a área de cibersegurança. Adicionalmente, foram realizadas leituras prévias dos títulos e resumos dos artigos para garantir a relevância dos documentos na análise final.

A análise final também utilizou o VOSviewer para identificar temas emergentes, principais autores e universidades mais produtivas no campo, oferecendo uma visão panorâmica do panorama atual da pesquisa em detecção de anomalias em sistemas críticos.

A revisão da literatura foi conduzida para analisar as técnicas mais recentes em detecção de anomalias, com ênfase no uso de aprendizado de máquina e inteligência artificial em sistemas de controle industrial.

Resultados e discussão

A natureza das ameaças cibernéticas varia significativamente entre diferentes regiões, exigindo análises específicas para cada contexto. Incidentes cibernéticos examinados na África do Sul, destacam a necessidade de adaptar estratégias de segurança às condições locais e regionais, através da diversidade de países que buscam inovações na área de segurança através da pesquisa, o que ressalta a variedade e complexidade das ameaças cibernéticas globais. (PIETERSE, 2021).

1. Liderança e Impacto por País

Uma análise mais detalhada dos dados aponta que o Estados Unidos da América (EUA) lidera em termos de número de documentos e citações como sugere a tabela, refletindo um investimento significativo e uma priorização na pesquisa de cibersegurança.

A Arabia Saudita e a Austrália também se destacam como grandes contribuidores, apesar do número de artigos e citações não serem os maiores, esses países possuem uma força de link (Total link strength) muito forte, que é o peso que a ferramenta VOSviewer usa para quantificar a relevância dos nós do grafo.

Tabela 01: Países

País	Documentos	Citações	Força do Link
USA	**21**	**233**	**10**
Saudi Arabia	**7**	**36**	**7**
Australia	**3**	**208**	**6**
Canada	**5**	**92**	**6**
Germany	**11**	**82**	**6**

2. Métodos de Detecção de Anomalias de Tráfego

Os métodos de detecção de anomalias em sistemas críticos incluem técnicas baseadas em aprendizado de máquina, como redes neurais profundas (Deep Neural Network - DNNs) e redes neurais convolucionais (Convolutional Neural Network - CNNs), é possível ver na análise da ferramenta que esses termos estavam em alta entre 2021.8 e 2022. A utilização de algoritmos de próxima geração para analisar dados de tráfego de rede e

identificar padrões que indicam eventos raros de segurança cibernética foi destacada por (ZHANG; COSTA-PEREZ; PATRAS, 2022).

3. Impacto da Inteligência Artificial e Aprendizado de Máquina

A adoção de técnicas avançadas de inteligência artificial se tornou importante, especialmente redes neurais convolucionais (ConvNet). Destaca-se o modelo TL-ConvNet, que utiliza transferência de conhecimento para melhorar a detecção de intrusões, demonstrando melhorias significativas em precisão nos conjuntos de dados NSL-KDD (WU; GUO; BUCKLAND, 2019).

4. Conexões Internacionais e Colaborações

A rede de colaboração entre países destaca-se no mapa, mostrando que países como a China, Estados Unidos e Índia não apenas produzem uma grande quantidade de pesquisa, mas também mantêm fortes laços de colaboração com outras nações. A interação entre esses e outros países, como Arábia Saudita e Austrália, sugere uma grande troca de conhecimento e recursos, que proporciona um avanço global constante da cibersegurança.

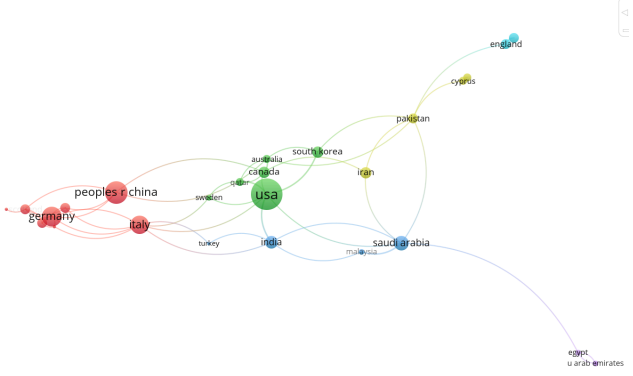

Figura 1: Conexão entre Países

Conclusões

Este estudo forneceu uma visão bem definida em áreas de estudo do estado da arte em ferramentas de detecção de anomalias em sistemas críticos, destacando a importância da cibersegurança em um cenário global em rápida evolução.

A pesquisa revelou que técnicas de aprendizado de máquina, como redes neurais profundas (DNNs) e redes neurais convolucionais (CNNs), estão se tornando cada vez mais relevantes na detecção de ameaças cibernéticas, com taxas de detecção impressionantes que superam 94% em alguns casos. Essa evolução tecnológica é crucial para o enfrentamento das ameaças emergentes em um mundo interconectado.

Por fim, as recomendações para pesquisas futuras incluem a exploração de novas tecnologias, como blockchain e privacidade diferencial, para aprimorar as técnicas de detecção de anomalias. Este trabalho contribui para o campo da cibersegurança, propondo um caminho para a evolução contínua das práticas e ferramentas de proteção de sistemas críticos.

Referências

CHIGADA, J.; MADZINGA, R. Cyberattacks and threats during covid-19: A systematic
literature review. South African Journal of Information Management, AOSIS Publishing, v. 23,
n. 1, p. 1–11, 2021. Citado na página 18.

PIETERSE, H. The cyber threat landscape in south africa: A 10-year review. The African
Journal of Information and Communication, Authors, v. 28, p. 1–21, 2021. Citado 3 vezes nas
páginas 17, 18 e 23.

CHIGADA, J.; MADZINGA, R. Cyberattacks and threats during covid-19: A systematic
literature review. South African Journal of Information Management, AOSIS Publishing, v. 23,
n. 1, p. 1–11, 2021. Citado na página 18.

YOU, L.; WANG, Z. A cloud based network intrusion detection system. Tehnički vjesnik,
Strojarski fakultet u Slavonskom Brodu; Fakultet elektrotehnike, računarstva . . . , v. 29, n. 3, p.
987–992, 2022. Citado 4 vezes nas páginas 17, 18, 22 e 24.

Ortega-Fernandez, I., Sestelo, M., Burguillo, J. C., and Pi˜n´on-Blanco, C. (2023). Network intrusion
detection system for ddos attacks in ics using deep autoencoders. Wireless Networks, pages 1–17.

ZHANG, C.; COSTA-PEREZ, X.; PATRAS, P. Adversarial attacks against deep learning-based
network intrusion detection systems and defense mechanisms.

IEEE/ACM Transactions on
Networking, IEEE, v. 30, n. 3, p. 1294–1311, 2022. Citado 2 vezes nas páginas 23 e 24.

WU, P.; GUO, H.; BUCKLAND, R. A transfer learning approach for network intrusion
detection. In: IEEE. 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA).
[S.l.], 2019. p. 281–285. Citado 2 vezes nas páginas 17 e 22.