Detecção de anomalias em redes de computadores utilizando Redes Adversárias Generativas

Vitor Gabriel da Silva Ruffo[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

vitor.gs.ruffo@gmail.com, proenca@uel.br

Abstract. *In the past few years, many tasks performed by human beings have been eased or automatized by computer networks. Those systems provide high value to society, and as a consequence, are targeted by malicious agents whose goal is to deny their offered services through anomalous events injection. A highly-accepted countermeasure that has been widely studied in the literature is the Deep Learning-based Network Intrusion Detection System (NIDS). Thus, this work aims to study the applicability of the Generative Adversarial Network (GAN), a Deep Learning method, in implementing a NIDS.*

Resumo. *Nos últimos anos, muitas das tarefas realizadas pelo ser humano têm sido facilitadas ou automatizadas com o uso de redes de computadores. Esses sistemas entregam um grande valor para a sociedade, e com isso, são alvos de agentes maliciosos que objetivam negar os seus serviços através da inserção de eventos anômalos. Uma medida altamente aceita e estudada na literatura para conter esses agentes e preservar o valor das redes são os Sistemas de Detecção de Intrusão de Redes baseados em Aprendizado Profundo. Deste modo, este trabalho propõe-se estudar a aplicabilidade de Rede Adversária Generativa, uma técnica de Aprendizado Profundo, na implementação de um desses sistemas.*

1. Introdução

Nos últimos anos, muitas tarefas realizadas pelo ser humano têm sido facilitadas ou automatizadas com o uso de redes de computadores. Exemplos dessas tarefas incluem transmissão de filmes e séries via internet, digitalização de contas bancárias e transferências via PIX [19], comunicação interpessoal, trabalho e estudo a distância, veículos autônomos, casas e cidades inteligentes, entre outros [69], [64], [21], [5].

Por estar tão presente no dia a dia das pessoas deste século, os serviços fornecidos pelas redes de computadores possuem um alto valor e a sua falha pode causar enormes prejuízos [4], [51]. Geralmente, essas falhas são produto de diversos tipos de comportamentos inexperados e fora do padrão que podem ocorrer no tráfego desses sistemas, as chamadas anomalias [22].

Nem toda anomalia é causada por um agente malicioso, como as decorrentes de falha de hardware, de software ou humana. Porém, é muito comum a ocorrência de ataques de redes, que são atividades anômalas causadas por usuários mal-intencionados com o intuito de comprometer a confidencialidade, integridade ou disponibilidade do sistema [22], [26], [7]. Por exemplo, recentemente, um ataque abalou um sistema importante de redes de computadores da Albânia, obrigando as autoridades a desliga-lo e impedindo o

fornecimento de serviços públicos on-line para os moradores do país [6]. Assim, é de extrema importância a construção de meios para garantir a proteção e o funcionamento adequado desses sistemas.

Uma abordagem de solução altamente aceita e estudada na comunidade científica para promover a segurança contra ataques de redes são os Sistemas de Detecção de Intrusão de Redes (NIDS) [65], [44], [48], [23], [34], [32], [27]. Esses sistemas agem monitorando o tráfego e gerando um aviso para o gerente de rede quando vestígios de comportamento anômalo são identificados. Seu principal objetivo é o oposto dos agentes maliciosos: manter a confidencialidade, integridade e disponibilidade do serviço de rede [22].

Entre os metódos utilizados na literatura na implementação de um NIDS, Aprendizado de Máquina tem se destacado devido aos bons resultados apresentados [41], [55]. Exemplos deste método incluem K-Vizinhos Mais Próximos, Árvore de Decisão, e Rede Neural [17]. Dentro desta área, as abordagens que mais têm ganhado atenção são as de Aprendizado Profundo [54], [20], que são tipos especiais de Rede Neural. Por exemplo, *Long Short-Term Memory (LSTM)* [46], *Convolutional Neural Network (CNN)* [13], *Auto-Encoder (AE)*, *Restricted Boltzmann Machine (RBM), Deep belief network (DBN)* e *Gated Recurrent Unit (GRU)* [1]. Uma técnica de Aprendizado Profundo concebida há não muito tempo atrás e que tem se mostrado promissora é a Rede Adversária Generativa (GAN) [47], [45].

Apesar da área de detecção de anomalias de redes ja ser estudada há muitos anos pela comunidade científica, o problema em questão ainda não foi completamente resolvido. Existem muitos pontos que ainda precisam ser tratados de uma melhor maneira, como é destacado em [70], [28], [22]. Deste modo, este trabalho propõe-se a estudar a aplicação de GAN na implementação de um NIDS.

O restante deste documento esta organizado da seguinte forma: a seção dois apresenta os conceitos, métodos e técnicas, além da revisão do estado da arte, necessários para a elaboração da proposta a ser desenvolvida. Na seção três é apresentado o objetivo a ser atingido ao fim do desenvolvimento. A seção quatro apresenta o passo a passo de como os conhecimentos descritos na seção dois serão usados para atingir o objetivo do trabalho. Em seguida, na seção cinco tem-se o cronograma de execução das atividades mencionadas na seção anterior. E, por fim, as contribuições do trabalho são descritas na seção seis.

2. Fundamentação Teórico-Metodológica e Estado da Arte

2.1. Anomalias de redes de computadores

Antes de desenvolver uma solução é necessário que não haja dúvidas em relação ao problema que se pretende resolver. Portanto, inicialmente, um estudo sobre a ideia de anomalias é essencial.

Deste modo, considere um conjunto de observações, onde cada uma delas é composta por um certo número de características. Uma observação é dita anômala quando as suas características destoam muito do padrão presente nas características das demais observações [22]. Por exemplo, a figura 1 ilustra um conjunto de pontos (observações) dispostos em um plano cartesiano. Esses pontos são formados por coordenadas x e y

(características). Pode-se observar que o padrão de comportamento de uma observação é estar disposta próximo a reta traçada em verde. O ponto destacado em vermelho é uma anomalia pois suas coordenadas desviam desse padrão, aumentando ligeiramente a sua distância entre a reta.

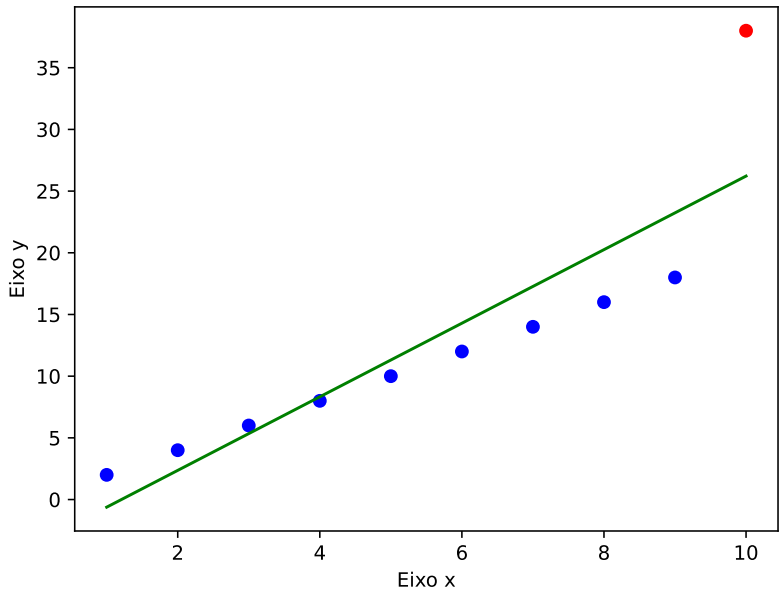

Figura 1. Exemplo de anomalia

Na área de gerência de redes de computadores, é comum a coleta de dados sobre o tráfego de rede afim de efetuar análises de seu comportamento [57]. A maioria das observações coletadas tendem a seguir um certo padrão e quando uma delas não o segue diz-se que esta é uma anomalia de rede. Existem diversos tipos de anomalias de redes que possuem características e causas diferentes [22].

Os dados de tráfego de rede podem ser coletados em diferentes formatos dependendo do mecanismo utilizado, como por exemplo *TCP dump, SNMP* e *IP Flow*. É de suma importância selecionar um formato de coleta de dados que seja capaz de capturar vestígios de ocorrência dos tipos de anomalias que se deseja detectar. Pois, diferentes tipos de anomalia podem afetar diferentes aspectos do tráfego de rede, e caso o formato de coleta não capture esses aspectos as anomalias alvo da análise não poderão ser identificadas [22].

2.2. Detecção de anomalias de redes de computadores

Uma das soluções mais aceitas para a detecção de anomalias de redes são os Sistemas de Detecção de Intrusão de Redes (NIDS). Esses sistemas são responsáveis por monitorar o tráfego e alertar os gerentes de redes quando rastros anômalos forem identificados [1]. Eles agem como uma segunda linha de defesa de redes contra ações maliciosas não capturadas pelos *firewalls*. Seu principal objetivo é preservar a confidencialidade, integridade e disponibilidade de redes de computadores [22]. Um detalhe importante que é considerado pelos cientistas é que a todo momento os ataques existentes evoluem e novos ataques são

concebidos [37], a fim de evitar a sua detecção. Assim, é importante que esses sistemas consigam se adaptar e evoluir para conseguirem detectar os novos tipos de ataque. Outro aspecto avaliado é que um NIDS precisa ter uma resposta rápida na detecção da presença de ataques [14], de modo a minimizar os prejuízos causados ao sistema.

Esses sistemas podem ser classificados de acordo com a estratégia de detecção utilizada. As duas mais comuns são a baseada em assinatura e a baseada em anomalia [70], [1]. Um NIDS implementado utilizando a primeira estratégia mantém um banco de dados contendo padrões de anomalias ja conhecidos. Assim, o seu trabalho se resume a monitorar o tráfego de rede tentando identificar algum desses padrões anômalos nos dados [37]. Uma vantagem desse método é que a taxa de falsos positivos é baixa, ja que o sistema só gera um alarme quando uma anomalia realmente for identificada [22]. A principal desvantagem dessa abordagem é que anomalias desconhecidas não são possiveis de serem identificadas, podendo causar uma alta taxa de falsos negativos [17]. Além disso, o banco de dados precisa ser constantemente atualizado pois é comum o surgimento de variações de anomalias conhecidas e de novas anomalias, o que pode ser uma tarefa custosa [1].

Ja um NIDS que faz uso da segunda abordagem constroe um modelo que representa o comportamento normal do tráfego utilizando dados históricos [22]. Deste modo, o seu trabalho é o de monitorar o tráfego comparando o comportamento observado com o comportamento normal ou esperado. Assim, uma anomalia é identificada quando o comportamento observado desvia muito do esperado [17]. A vantagem desse método é que ele torna o sistema capaz de identificar anomalias desconhecidas, além das conhecidas [22]. Porém, sua principal desvantagem é que esse tipo de abordagem tende a gerar uma alta taxa de falsos positivos [37]. Isso ocorre porque qualquer variação não maliciosa no comportamento do tráfego é considerada como anomalia, o que é comum pois o comportamento normal de uma rede pode variar de tempos em tempos. Assim, é necessário que o modelo de comportamento normal seja atualizado constantemente e essa tarefa pode ter um custo elevado [22]. Esse tipo de NIDS é o mais utilizado e estudado na literatura e será a estratégia que será adotada na construção do sistema deste trabalho.

Existe um grande esforço em meio a comunidade científica na construção de um Sistema de Detecção de Intrusão de Redes que atenda a todas as necessidades de segurança. Deste modo, inumeros trabalhos têm sido publicados ao longo dos anos. Um exemplo desse esforço pode ser observado no grupo de pesquisa ORION da Universidade Estadual de Londrina, que tem contribuido desde 2004 para o avanço da ciência nessa área do conhecimento [52], [8], [10], [15], [53], [50], [29], [9], [59]. Entre os seus diversos trabalhos publicados pode-se destacar [22], onde os autores realizaram uma revisão de literatura, apresentando uma visão vasta do estado da arte e diversos conceitos fundamentais. Outro trabalho importante publicado pelo grupo é [29], que propõe um NIDS baseado em anomalias autônomo e não-supervisionado. Esse sistema é implementado com o uso de Algoritmos Genéticos para a geração do modelo de comportamento normal, e Lógica Difusa no algoritmo de detecção de anomalias. [13] desenvolveu um NIDS baseado em anomalias utilizando CNN para ambientes de Internet das Coisas.

2.3. Aprendizado de Máquina

Existem muitas tarefas para as quais é extremamente difícil especificar algoritmos que as resolvam [43]. Porém, nos dias de hoje, existe uma enorme quantidade de dados que

podem auxiliar na construção desses algoritmos [2]. Por exemplo, não há um algoritmo para determinar se um e-mail é spam ou não, porém existe uma grande quantidade de exemplos de e-mails considerados spam ou legítimos [2]. Assim, uma solução para a categorização de e-mails seria aquela em que o sistema fosse capaz de derivar automaticamente uma aproximação de algoritmo para esse problema a partir dos dados referente a eles [2]. Esse tipo de solução é chamada de Aprendizado de Máquina (ML), uma subárea de Inteligência Artificial (AI) [24] como apresentado na figura 2.

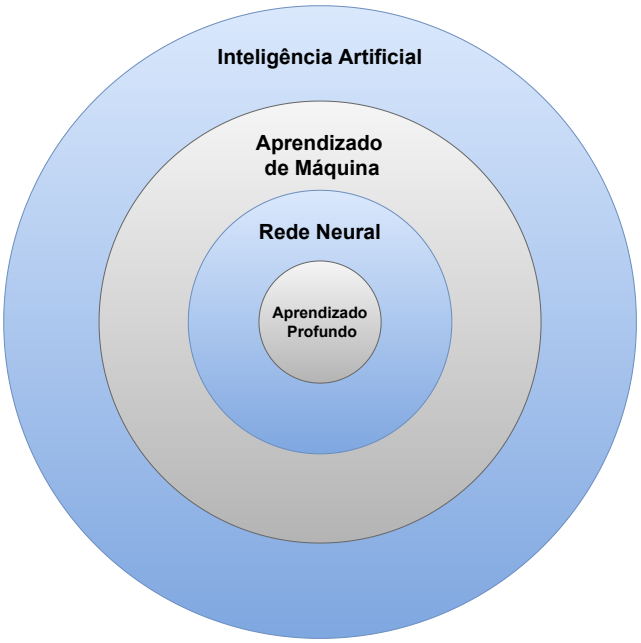

Figura 2. Relação entre as áreas de aprendizado

Aprendizado de Máquina é uma método computacional para a construção de sistemas que aprendem a performar uma tarefa sobre um conjunto de dados [42], [43]. Inicialmente, o sistema treina a realização da tarefa com o uso de um conjunto de dados de treinamento. Assim, durante o treinamento o sistema melhora automaticamente na realização da tarefa através de experiência [33]. Após o treino, espera-se que o sistema seja capaz de executar a mesma tarefa para conjuntos de dados que ele ainda não teve contato. No caso do problema de categorização de e-mails, o sistema aprenderia a realizar a categorização analisando os dados sobre e-mails ja categorizados e entendo os seus padrões. Após isso, o sistema estaria pronto para categorizar e-mails que ele nunca analisou antes.

2.3.1. Tipos de aprendizado

As técnicas de Aprendizado de Máquina podem ser classificadas em três principais tipos: supervisionada, semi-supervisionada e não-supervisionada [43], [67], [68]. A principal diferença entre essas formas de aprendizado esta presente nos dados que são utilizados no treinamento [30]. Técnicas supervisionadas utilizam em seu treinamento um conjunto

de dados onde cada observação X possui um rótulo Y que a descreve [68]. Assim, seu objetivo é o de aprender uma função f que mapeie um X qualquer para um Y' que seja satisfatóriamente próximo do Y real [43]. Esse tipo de ML é utilizado para resolver problemas de classificação e de regressão e pode ser implementada utilizando diversos algoritmos como K-vizinhos Mais Próximos, Arvore de Decisão, Floresta Aleatória, Rede Neural e Máquina de Vetores de Suporte [67].

A tarefa de rotulação é extremamente custosa e com isso, geralmente, grande parte das observações dos conjuntos de dados disponíveis estão sem rótulo [67], [43]. Técnicas semi-supervisionadas procuram utilizar observações com e sem rótulo no processo de treinamento [68]. Deste modo, seu objetivo é de utilizar os dados não rotulados para construir um sistema supervisionado que seja melhor do que aquele que seria construido utilizando somente os poucos dados rotulados disponíveis [43].

Técnicas não supervisionadas fazem uso de conjuntos de dados cujas observações não possuem rótulo. O objetivo básico desse tipo de técnica é encontrar padrões e estruturas que estão escondidos nos dados [43], [67], [68]. Elas geralmente são utilizadas para resolver problemas de clusterização e redução de dimensionalidade e podem ser implementadas utilizando algoritmos como Rede Neural, Agrupamento k-means, Mapas de Kohonen, Análise de Componentes Principais [42].

2.3.2. Rede Neural

Rede Neural (NN) é um algoritmo famoso de Aprendizado de Máquina que pode ser implementado para cada uma das categorias de aprendizado [42]. A ideia por trás do algoritmo é inspirada no cérebro humano e utiliza unidades chamadas de neurônios e suas interconexões para efetuar cálculos complexos [67], [43]. Uma NN é formada por camadas sequenciais de neurônios, onde neurônios de camadas adjacentes podem estabelecer conexões. A primeira camada, a de entrada, recebe os dados de entrada (propriedades de uma observação). A última camada representa a saída Y calculada para a entrada X alimentada na primeira camada. Entre as camadas de entrada e saída existe uma camada escondida. Deste modo, inumeras variações de NN podem ser construídas ao variar o número de neurônios em cada camada e o número de camadas escondidas [67].

2.3.3. Aprendizado Profundo

Aprendizado Profundo (DL) é uma técnica de Aprendizado de Máquina que vem ganhando popularidade nos últimos anos devido a sua aplicabilidade na solução de problemas em diversas áreas [62], [35]. Basicamente, DL é uma subárea de ML (figura 2) e estuda um tipo mais poderoso de Rede Neural que possui múltiplas camadas escondidas, chamada de Rede Neural Profunda (DNN) [30], [37], [1]. Uma DNN é capaz de modelar conceitos e funções bem mais complexas do que uma simples Rede Neural [62], [24], [1], e com isso, são capazes de resolver problemas mais difíceis.

Em meio as diferenças entre Aprendizado de Máquina e Aprendizado Profundo pode-se citar [37]: DL requer um grande volume de dados de treinamento, enquanto que ML não; Diferente de ML, as técnicas de DL efetuam a engenharia de características dos

dados de maneira automática, reduzindo a intervenção humana; DL requer mais poder e recursos computacionais do que ML.

As diferentes arquiteturas de DNN podem ser classificadas em discriminativas, generativas e híbridas [1]. As primeiras arquiteturas se referem a uma DNN que segue um treinamento supervisionado [62], como por exemplo a CNN. As generativas dizem respeito as redes cujo treinamento ocorre de maneira não supervisionada, enquanto que as hibridas apresentam arquiteturas que combinam os dois tipos de aprendizado. Exemplos de arquiteturas generativas incluem *Autoencoder (AE)* e *Recurrent Neural Network (RNN)* [1]. Um tipo de arquitetura híbrida encontrada na literatura é a GAN [62], que será estudada neste trabalho.

2.4. Rede Adversária Generativa

A Rede Adversária Generativa (GAN) representa uma nova arquitetura ou técnica de Aprendizado Profundo concebida no ano de 2014 por *Goodfellow et al*. [25]. Esse tipo de DL é baseado na Teoria do Jogos e é composta por duas redes neurais internas que competem entre si, o gerador e o discriminador [45]. O gerador é treinado para gerar exemplos de dados sintéticos e enganar o discriminador. Ja o discriminador aprende a dicernir exemplos falsos criados pelo gerador dos exemplos reais de dados [58], [39]. O objetivo final é obter uma rede geradora que é capaz de enganar totalmente a discriminadora, ou seja, a rede discriminadora não ser mais capaz de indicar se um exemplo é sintético ou real. Quando esse objetivo é atingido obtém-se um gerador que aprendeu a distribuição dos dados e é capaz de gerar exemplos muito parecidos com os reais [49], [45].

Como GAN é um tipo de modelo generativo, uma de suas principais aplicações é a de geração de dados [49]. O trabalho descrito em [66] utiliza CNN para detectar a infecção por COVID-19 em pacientes com base em imagens raio-x da região peitoral. Os autores destacam que a falta de imagens para efetuar o treinamento da rede reduz a seu desempenho de detecção. Assim, eles utilizaram uma GAN para gerar imagens sintéticas e aumentar o conjunto de dados de treinamento da rede. Outra area de aplicação que as GANs têm tido bons resultados é a de Visão Computacional. [16] utilizaram essas redes na construção de um sistema que tem como entrada uma imagem de uma pessoa utilizando máscara e produz como saída uma imagem próxima da realidade dessa mesma pessoa sem a máscara. Alguns trabalhos também ja utilizaram GANs na tarefa de detecção de anomalias [36], [61].

A Rede Adversária Generativa também têm se mostrado útil na construção de Sistemas de Detecção de Intrusão de Redes. Muitos desses trabalhos têm utilizando GAN para gerar exemplos de dados sintéticos e resolver o problema de desbalanceamento de classes [31], [18], [11], [63], [12], [3], [56]. Esse problema prejudica a performance dos algoritmos de Aprendizado de Máquina e precisa ser tratado para garantir um treinamento de qualidade [40].

3. Objetivos

O objetivo deste trabalho é estudar Redes Adversárias Generativas (GANs) e a sua viabilidade na implementação de um Sistema de Detecção de Anomalias em Redes Definidas por Software.

4. Procedimentos metodológicos/Métodos e técnicas

Primeiramente, as aplicações gerais de GAN serão estudadas. Depois, o escopo de estudo será reduzido, considerando apenas trabalhos que utilizam GANs no processo de detecção de anomalias em redes de computadores. Em seguida, haverá a implementação de um NIDS baseado em GAN. O sistema será testado e depurado utilizando os dados sintetizados pelo grupo de pesquisa ORION da Universidade Estadual de Londrina [60]. Por fim, a performance do modelo proposto será comparada com a de um trabalho similar, como aquele apresentado por Lent *et al.* [38], utilizando os mesmos dados citados anteriormente.

5. Cronograma de Execução

Nessa seção são listadas as atividades descritas na seção anterior. Além disso, um cronograma para execução das mesmas também é proposto, como apresentado na tabela 1.

Atividades:

1. Estudo das aplicações de GAN;
2. Estudo de GAN aplicada especificamente na área de detecção de anomalias em redes de computadores;
3. Desenvolvimento de um NIDS baseado em GAN;
4. Teste de performance e depuração do NIDS;
5. Comparação de performance entre o sistema desenvolvido e um similar;
6. Escrita TCC (versão preliminar);
7. Escrita TCC (versão para a banca examinadora).

Tabela 1. Cronograma de Execução

	ago	set	out	nov	dez	jan	fev	mar	abr
Atividade 1	X	X	X						
Atividade 2		X	X	X	X				
Atividade 3			X	X	X	X			
Atividade 4					X	X	X		
Atividade 5							X	X	
Atividade 6		X	X	X	X	X			
Atividade 7							X	X	X

6. Contribuições e/ou Resultados esperados

Espera-se poder indicar se as redes GAN são um modelo viável na implementação de um NIDS. Além disso, pretende-se apresentar um relatório de comparação de eficiência entre o NIDS implementado com redes GAN e um construído com uma outra técnica de Aprendizado Profundo, como proposto por Lent *et al.* [38]. Essa comparação será feita utilizando o conjunto de dados gerado pelo grupo de pesquisa ORION da Universidade Estadual de Londrina [60].

7. Espaço para assinaturas

Londrina, *12 de Setembro de 2022*.

_____	_____
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. URL: https://doi.org/10.1016/j.knosys.2019.105124.

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

[3] Giuseppina Andresini, Annalisa Appice, Luca De Rose, and Donato Malerba. Gan augmentation to deal with imbalance in imaging-based intrusion detection. *Future Generation Computer Systems*, 123:108–127, 2021. URL: https://doi.org/10.1016/j.future.2021.04.017.

[4] Eirini Anthi, Lowri Williams, Małgorzata Słowińska, George Theodorakopoulos, and Pete Burnap. A supervised intrusion detection system for smart home iot devices. *IEEE Internet of Things Journal*, 6(5):9042–9053, 2019. URL: https://doi.org/10.1109/JIOT.2019.2926365.

[5] 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. URL: https://doi.org/10.1016/j.jnca.2020.102942.

[6] BalkanInsight. Albania blames 'massive cyber attack' as govt servers go down. https://balkaninsight.com/2022/07/18/albania-gov-says-it-is-being-attacked-as-service-servers-are-down/. Accessed: 2022-08-19.

[7] Punam Bedi, Neha Gupta, and Vinita Jindal. Siam-ids: Handling class imbalance problem in intrusion detection systems using siamese neural network. *Procedia Computer Science*, 171:780–789, 2020. URL: https://doi.org/10.1016/j.procs.2020.04.085.

[8] 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. URL: https://doi.org/10.1109/ICC.2017.7997214.

[9] Luiz Fernando Carvalho, Taufik Abrão, Leonardo de Souza Mendes, and Mario Lemes Proença Jr. An ecosystem for anomaly detection and mitigation in software-defined networking. *Expert Systems with Applications*, 104:121–133, 2018. URL: https://doi.org/10.1016/j.eswa.2018.03.027.

[10] Luiz Fernando Carvalho, Sylvio Barbon Jr, Leonardo de Souza Mendes, and Mario Lemes Proenca Jr. Unsupervised learning clustering and self-organized agents applied to help network management. *Expert Systems with Applications*, 54:29–47, 2016. URL: https://doi.org/10.1016/j.eswa.2016.01.032.

[11] Marc Chalé and Nathaniel D Bastian. Generating realistic cyber data for training and evaluating machine learning classifiers for network intrusion detection systems. *Expert Systems with Applications*, page 117936, 2022. URL: https://doi.org/10.1016/j.eswa.2022.117936.

[12] Radhika Chapaneri and Seema Shah. Enhanced detection of imbalanced malicious network traffic with regularized generative adversarial networks. *Journal of Network*

and Computer Applications, 202:103368, 2022. URL: https://doi.org/10.1016/j.jnca.2022.103368.

[13] 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. URL: https://doi.org/10.1016/j.compeleceng.2020.106738.

[14] 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. URL: https://doi.org/10.1109/ACCESS.2018.2878576.

[15] Marcos VO De Assis, Joel JPC Rodrigues, and Mario Lemes Proença. A novel anomaly detection system based on seven-dimensional flow analysis. In *2013 IEEE Global Communications Conference (GLOBECOM)*, pages 735–740. IEEE, 2013. URL: https://doi.org/10.1109/GLOCOM.2013.6831160.

[16] Nizam Ud Din, Kamran Javed, Seho Bae, and Juneho Yi. A novel gan-based network for unmasking of masked face. *IEEE Access*, 8:44276–44287, 2020. URL: https://doi.org/10.1109/ACCESS.2020.2977386.

[17] Ayesha S Dina and D Manivannan. Intrusion detection based on machine learning techniques in computer networks. *Internet of Things*, 16:100462, 2021. URL: https://doi.org/10.1016/j.iot.2021.100462.

[18] Hongwei Ding, Leiyang Chen, Liang Dong, Zhongwang Fu, and Xiaohui Cui. Imbalanced data classification: A knn and generative adversarial networks-based hybrid approach for intrusion detection. *Future Generation Computer Systems*, 131:240–254, 2022. URL: https://doi.org/10.1016/j.future.2022.01.026.

[19] Banco Central do Brasil. O que é pix? https://www.bcb.gov.br/estabilidadefinanceira/pix. Accessed: 2022-08-19.

[20] Mahmoud Said ElSayed, Nhien-An Le-Khac, Marwan Ali Albahar, and Anca Jurcut. A novel hybrid model for intrusion detection systems in sdns based on cnn and a new regularization technique. *Journal of Network and Computer Applications*, 191:103160, 2021. URL: https://doi.org/10.1016/j.jnca.2021.103160.

[21] Mojtaba Eskandari, Zaffar Haider Janjua, Massimo Vecchio, and Fabio Antonelli. Passban ids: An intelligent anomaly-based intrusion detection system for iot edge devices. *IEEE Internet of Things Journal*, 7(8):6882–6897, 2020. URL: https://doi.org/10.1109/JIOT.2020.2970501.

[22] 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(3):447–489, 2019. URL: https://doi.org/10.1007/s11235-018-0475-8.

[23] Xianwei Gao, Chun Shan, Changzhen Hu, Zequn Niu, and Zhen Liu. An adaptive ensemble machine learning model for intrusion detection. *IEEE Access*, 7:82512–82521, 2019. URL: https://doi.org/10.1109/ACCESS.2019.2923640.

[24] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep learning*. MIT press, 2016. URL: https://doi.org/10.4258/hir.2016.22.4.351.

[25] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. *Advances in neural information processing systems*, 27, 2014. URL: https://doi.org/10.48550/arXiv.1406.26617.

[26] Neha Gupta, Vinita Jindal, and Punam Bedi. Lio-ids: handling class imbalance using lstm and improved one-vs-one technique in intrusion detection system. *Computer Networks*, 192:108076, 2021. URL: https://doi.org/10.1016/j.comnet.2021.108076.

[27] Neha Gupta, Vinita Jindal, and Punam Bedi. Cse-ids: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems. *Computers & Security*, 112:102499, 2022. URL: https://doi.org/10.1016/j.cose.2021.102499.

[28] Somayye Hajiheidari, Karzan Wakil, Maryam Badri, and Nima Jafari Navimipour. Intrusion detection systems in the internet of things: A comprehensive investigation. *Computer Networks*, 160:165–191, 2019. URL: https://doi.org/10.1016/j.comnet.2019.05.014.

[29] 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. URL: https://doi.org/10.1016/j.eswa.2017.09.013.

[30] William Grant Hatcher and Wei Yu. A survey of deep learning: Platforms, applications and emerging research trends. *IEEE Access*, 6:24411–24432, 2018. URL: https://doi.org/10.1109/ACCESS.2018.2830661.

[31] Shuokang Huang and Kai Lei. Igan-ids: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks. *Ad Hoc Networks*, 105:102177, 2020. URL: https://doi.org/10.1016/j.adhoc.2020.102177.

[32] Sana Ullah Jan, Saeed Ahmed, Vladimir Shakhov, and Insoo Koo. Toward a lightweight intrusion detection system for the internet of things. *IEEE Access*, 7:42450–42471, 2019. URL: https://doi.org/10.1109/ACCESS.2019.2907965.

[33] Michael I Jordan and Tom M Mitchell. Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245):255–260, 2015. URL: https://doi.org/10.1126/science.aaa8415.

[34] 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. URL: https://doi.org/10.1109/ACCESS.2019.2899721.

[35] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton. Deep learning. *nature*, 521(7553):436–444, 2015. URL: https://doi.org/10.1038/nature14539.

[36] 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. URL: https://doi.org/10.1109/ACCESS.2021.3078553.

[37] 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. URL: https://doi.org/10.1016/j.jnca.2021.103111.

[38] 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. URL: https://doi.org/10.1109/ACCESS.2022.3190008.

[39] 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. URL: https://doi.org/10.1016/j.neucom.2020.12.114.

[40] Xu Liu, Xiaoqiang Di, Qiang Ding, Weiyou Liu, Hui Qi, Jinqing Li, and Huamin Yang. Nads-ra: network anomaly detection scheme based on feature representation and data augmentation. *IEEE Access*, 8:214781–214800, 2020. URL: https://doi.org/10.1109/ACCESS.2020.3040510.

[41] Wei Lo, Hamed Alqahtani, Kutub Thakur, Ahmad Almadhor, Subhash Chander, and Gulshan Kumar. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. *Vehicular Communications*, 35:100471, 2022. URL: https://doi.org/10.1016/j.vehcom.2022.100471.

[42] Panos Louridas and Christof Ebert. Machine learning. *IEEE Software*, 33:110–115, 09 2016. URL: https://doi.org/10.1109/MS.2016.114.

[43] Mohssen Mohammed, Muhammad Badruddin Khan, and Eihab Bashier Mohammed Bashier. *Machine learning: algorithms and applications*. Crc Press, 2016. URL: https://doi.org/10.1201/9781315371658.

[44] Nour Moustafa, Benjamin Turnbull, and Kim-Kwang Raymond Choo. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. *IEEE Internet of Things Journal*, 6(3):4815–4830, 2018. URL: https://doi.org/10.1109/JIOT.2018.2871719.

[45] 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. URL: https://doi.org/10.1016/j.comnet.2021.108149.

[46] Matheus P Novaes, Luiz F Carvalho, Jaime Lloret, and Mario Lemes Proença. Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. *IEEE Access*, 8:83765–83781, 2020. URL: https://doi.org/10.1109/ACCESS.2020.2992044.

[47] 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. URL: https://doi.org/10.1016/j.future.2021.06.047.

[48] Hamed Haddad Pajouh, Reza Javidan, Raouf Khayami, Ali Dehghantanha, and Kim-Kwang Raymond Choo. A two-layer dimension reduction and two-tier classi-

fication model for anomaly-based intrusion detection in iot backbone networks. *IEEE Transactions on Emerging Topics in Computing*, 7(2):314–323, 2016. URL: https://doi.org/10.1109/TETC.2016.2633228.

[49] Zhaoqing Pan, Weijie Yu, Xiaokai Yi, Asifullah Khan, Feng Yuan, and Yuhui Zheng. Recent progress on generative adversarial networks (gans): A survey. *IEEE Access*, 7:36322–36333, 2019. URL: https://doi.org/10.1109/ACCESS.2019.2905015.

[50] 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. URL: https://doi.org/10.1016/j.ins.2017.08.074.

[51] Sergio Iglesias Pérez, Santiago Moral-Rubio, and Regino Criado. A new approach to combine multiplex networks and time series attributes: Building intrusion detection systems (ids) in cybersecurity. *Chaos, Solitons & Fractals*, 150:111143, 2021. URL: https://doi.org/10.1016/j.chaos.2021.111143.

[52] M Lemes Proença, Camiel Coppelmans, Mauricio Bottoli, A Alberti, and Leonardo S Mendes. The hurst parameter for digital signature of network segment. In *International Conference on Telecommunications*, pages 772–781. Springer, 2004. URL: https://doi.org/10.1007/978-3-540-27824-5_103.

[53] 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. URL: https://doi.org/10.1002/nem.1892.

[54] Weicheng Qiu, Yinghua Ma, Xiuzhen Chen, Haiyang Yu, and Lixing Chen. Hybrid intrusion detection system based on dempster-shafer evidence theory. *Computers & Security*, 117:102709, 2022. URL: https://doi.org/10.1016/j.cose.2022.102709.

[55] K Narayana Rao, K Venkata Rao, and Prasad Reddy PVGD. A hybrid intrusion detection system based on sparse autoencoder and deep neural network. *Computer Communications*, 180:77–88, 2021. URL: https://doi.org/10.1016/j.comcom.2021.08.026.

[56] Markus Ring, Daniel Schlör, Dieter Landes, and Andreas Hotho. Flow-based network traffic generation using generative adversarial networks. *Computers & Security*, 82:156–172, 2019. URL: https://doi.org/10.1016/j.cose.2018.12.012.

[57] 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. URL: https://doi.org/10.1016/j.cose.2019.06.005.

[58] Afia Sajeeda and BM Mainul Hossain. Exploring generative adversarial networks and adversarial training. *International Journal of Cognitive Computing in Engineering*, 2022. URL: https://doi.org/10.1016/j.ijcce.2022.03.002.

[59] 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. URL: https://doi.org/10.1109/ACCESS.2020.2997939.

[60] 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. URL: https://doi.org/10.1109/ACCESS.2020.2997939.

[61] 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. URL: https://doi.org/10.1016/j.media.2019.01.010.

[62] Ajay Shrestha and Ausif Mahmood. Review of deep learning algorithms and architectures. *IEEE access*, 7:53040–53065, 2019. URL: https://doi.org/10.1109/ACCESS.2019.2912200.

[63] Aliya Tabassum, Aiman Erbad, Wadha Lebda, Amr Mohamed, and Mohsen Guizani. Fedgan-ids: Privacy-preserving ids using gan and federated learning. *Computer Communications*, 2022. URL: https://doi.org/10.1016/j.comcom.2022.06.015.

[64] Bayu Adhi Tama, Marco Comuzzi, and Kyung-Hyune Rhee. Tse-ids: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. *IEEE access*, 7:94497–94507, 2019. URL: https://doi.org/10.1109/ACCESS.2019.2928048.

[65] Ravi Vinayakumar, Mamoun Alazab, KP Soman, Prabaharan Poornachandran, Ameer Al-Nemrat, and Sitalakshmi Venkatraman. Deep learning approach for intelligent intrusion detection system. *Ieee Access*, 7:41525–41550, 2019. URL: https://doi.org/10.1109/ACCESS.2019.2895334.

[66] Abdul Waheed, Muskan Goyal, Deepak Gupta, Ashish Khanna, Fadi Al-Turjman, and Plácido Rogerio Pinheiro. Covidgan: data augmentation using auxiliary classifier gan for improved covid-19 detection. *Ieee Access*, 8:91916–91923, 2020. URL: http://dx.doi.org/10.1109/ACCESS.2020.2994762.

[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. URL: https://doi.org/10.1109/COMST.2018.2866942.

[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. URL: https://doi.org/10.1109/ACCESS.2018.2836950.

[69] Li Yang, Abdallah Moubayed, and Abdallah Shami. Mth-ids: a multitiered hybrid intrusion detection system for internet of vehicles. *IEEE Internet of Things Journal*, 9(1):616–632, 2021. URL: https://doi.org/10.1109/JIOT.2021.3084796.

[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*, page 102675, 2022. URL: https://doi.org/10.1016/j.cose.2022.102675.