UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CIÊNCIA DA COMPUTAÇÃO

Mariana dos Santos Dick

Aperfeiçoamentos do gerenciamento de segurança de sistema de detecção de intrusão para Internet of Things com Fog Computing através da utilização de Machine Learning

Florianópolis
2022

RESUMO

A implementação de sistemas de detecção de intrusão é uma problemática central em redes IoT (*Internet of Things*), visto às limitações de recursos dos dispositivos agregados a ela. Para garantir integridade, disponibilidade e autenticidade na rede, é necessário detectar e classificar tentativas de intrusão. Métodos baseados em aprendizado de máquina supervisionado são comumente utilizados na literatura para solucionar o referido problema. Com base nisso, esse trabalho busca realizar uma revisão do estado da arte no contexto de métodos baseados em aprendizado de máquina para identificar e categorizar intrusões em ambientes de *Fog* e IoT, com o objetivo de identificar possíveis problemas e soluções.

1 INTRODUÇÃO

1.1. MOTIVAÇÃO E JUSTIFICATIVAS

A Internet das Coisas é um paradigma que tem transformado vidas, indústrias e o mundo de maneira significativa através da extração e da transferência de dados. Apesar de atuar como uma facilitadora, essa tecnologia traz consigo uma gama de desafios e vulnerabilidades, podendo se tornar um risco à segurança e à privacidade do usuário. A detecção de intrusão é o primeiro passo para impedir que ataques aconteçam. Contudo, os dispositivos *IoT* possuem baixa capacidade de processamento e armazenamento, o que torna as metodologias de segurança tradicionais inadequadas. A Inteligência Artificial é amplamente utilizada em sistemas de detecção de intrusão para Internet das Coisas e se mostra eficiente para essa finalidade. A partir disso, a principal motivação do presente trabalho é estudar abordagens para IDS baseadas em Machine Learning, a fim de identificar possíveis impasses e dificuldades enfrentadas, tal como possíveis soluções.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

O objetivo geral deste trabalho é realizar uma revisão do estado da arte em aperfeiçoamentos do gerenciamento de segurança de sistema de detecção de intrusão para Internet of Things com Fog Computing utilizando métodos de aprendizado de máquina supervisionada.

1.2.2 OBJETIVOS ESPECÍFICOS

- Realizar uma revisão do estado da arte em detecção e prevenção de intrusão em IoT e Computação em Névoa;
- Relacionar e discutir trabalhos correlatos, destacando os problemas e as soluções apresentadas;
- Indicar uma proposta de abordagem para uma das problemáticas elencadas.

1.3 ORGANIZAÇÃO DO ARTIGO

O trabalho é organizado nas seguintes seções: 1. introdução, 2. conceitos básicos, 3. trabalhos correlatos, 4. aspectos relevantes, 5. problemas existentes, 6. soluções possíveis e 7. referências bibliográficas. A seção 1 trata da motivação e dos objetivos do trabalho. Na seção 2 são descritos os principais conceitos acerca da problemática. Na seção 3 são apresentados os trabalhos correlatos, e nas seções 4, 5 e 6 os trabalhos lidos são discutidos, comentando, respectivamente, os aspectos mais importantes, possíveis problemas e soluções. A seção 7 apresenta as referências utilizadas.

2 CONCEITOS BÁSICOS

2.1 INTERNET OF THINGS (IOT)

A Internet das Coisas integra diversos objetos físicos através de uma rede, permitindo que interajam entre si de maneira autônoma. Dispositivos IoT podem utilizar a Internet para fornecer e coletar dados, levando a uma conectividade generalizada entre pessoas, serviços, sensores e objetos. Essa tecnologia possui um vasto conjunto de aplicações, desde monitoramento hospitalar até casas inteligentes, variando em propósito, tamanho e complexidade (CONTI et al., 2018).

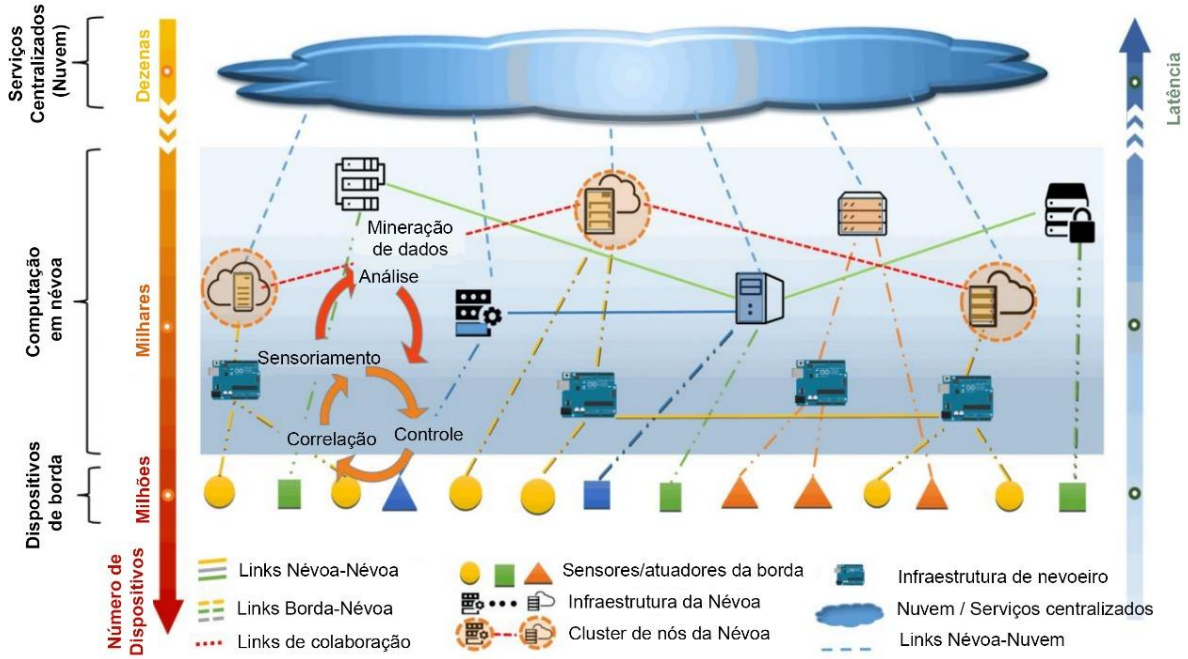
Os dispositivos IoT geralmente possuem estrutura simples e tamanho reduzido, com capacidade limitada de processamento e armazenamento. Dessa forma, é possível utilizar recursos computacionais de tecnologias independentes de domínio como a Computação em Nuvem para a execução de tarefas mais complexas, como tratamento de dados os (AL-FUQAHA et al., 2015).

2.3 FOG COMPUTING

A Computação em Névoa (*Fog Computing*) é uma plataforma altamente virtualizada que fornece serviços de armazenamento, processamento e rede entre dispositivos inteligentes e *Cloud Computing Data Centers* (BONOMI et al., 2012). Esse modelo se encontra na borda da rede, minimizando o tempo de resposta das requisições entre os dispositivos inteligentes e a *Cloud*. Dessa forma, a *Fog* facilita a implementação de aplicações e serviços distribuídos sensíveis à latência (IORGA et al., 2018).

A Figura 1 retrata como a *Fog Computing* pode auxiliar um ecossistema baseado em *Cloud* para atender dispositivos inteligentes. A *Fog* não é uma camada obrigatória no ecossistema, assim como a *Cloud* não é obrigatória para o atendimento das demandas dos dispositivos pela *Fog*. Dessa maneira, diferentes cenários de utilização podem requerer arquiteturas distintas, otimizadas de acordo com as necessidades da aplicação.

Figura 1 – Modelo de computação em névoa.



Fonte: Adaptado de Iorga et al. (2018).

3 TRABALHOS CORRELATOS

Com o objetivo de construir uma perspectiva do atual estado da arte em detecção e prevenção de intrusão em IoT e Computação em Névoa foi realizada uma revisão bibliográfica da literatura. Para isso foram pesquisados trabalhos científicos publicados a partir do ano de 2021 na base de artigos Elsevier. A partir dessa busca foram escolhidos alguns trabalhos que propõem diferentes técnicas de detecção baseadas em Machine Learning no contexto de ambientes IoT e de Computação em Névoa.

3.1 Revisão Bibliográfica Sistemática

Tabela 1 – Resultados das buscas por palavra-chave na base de pesquisa

“IoT”	17.549
“Internet of Things”	18.506
“Fog Computing”	1.682
“Intrusion Detection System”	1.340
“Machine Learning”	88.493

“Internet of Things” e “Fog Computing” e “Intrusion Detection System” e “Machine Learning”	127

A revisão foi realizada pesquisando pelas palavras-chaves nos anos a partir de 2021. É possível observar que, atualmente, Machine Learning é um tópico em alta e vem sendo altamente estudado. Porém, a utilização de Machine Learning para Sistemas de Detecção de Intrusão não possui tantos artigos, havendo a necessidade de maior concentração de esforços a fim de expandir a área e obter melhores resultados.

3.2 Intrusion detection using multi-objective evolutionary convolutional neural network for Internet of Things in Fog computing

Segundo Chen et al. (2022), o mundo está entrando rapidamente na era da Internet das Coisas (IoT), que conecta vários dispositivos a serviços digitais que facilitam muito nossas vidas. Com o rápido aumento no número de dispositivos conectados à IoT, mais vulnerabilidades de rede podem existir, levando a mais ataques cibernéticos. Nesse ambiente dinâmico de IoT, um sistema de detecção de intrusão (IDS) eficiente é urgentemente necessário para detectar ataques com baixa latência e alta precisão.

Vários IDSs promissores foram propostos com base em técnicas de aprendizado profundo (DL), mas eles precisam fazer ajustes de parâmetros em diferentes ambientes, o que consome muito tempo. Para amenizar esse problema, este artigo propõe uma rede neural convolucional evolutiva multiobjetivo para sistema de detecção de intrusão, chamada MECNN, que é executada nos nós de névoa da computação Fog em IoT. Nesta abordagem, a rede neural convolucional (CNN) é usada como classificador para detectar intrusões e o algoritmo evolutivo multiobjetivo baseado em decomposição (MOEA/D) é modificado para evoluir o modelo CNN, o que simplifica bastante o processo de ajuste de parâmetros de DL.

Isto é, um novo esquema de codificação é proposto primeiro para transformar a arquitetura topológica da CNN em um cromossomo de MOEA/D e, em seguida, os dois objetivos conflitantes, ou seja, desempenho de detecção e complexidade do modelo CNN, são simultaneamente otimizados pelo MOEA/D, que pode obter vários IDSs com vários desempenhos de detecção e complexidades de modelo. Então, o modelo MECNN mais adequado pode ser implantado em diferentes nós de névoa da computação Fog, fornecendo detecção de intrusão de baixa latência e alta precisão para IoT.

Por fim, os estudos experimentais são realizados em dois conjuntos de dados populares (AWID e CIC-IDS2107), que validaram que o modelo MECNN pode melhorar o desempenho e a robustez da detecção para proteger melhor a IoT quando comparado a outros IDSs de última geração.

3.3 Scalable machine learning-based intrusion detection system for IoT-enabled smart cities

Segundo Rahman et al. (2020), dada a escala crescente da IoT para permitir o gerenciamento sustentável de recursos em cidades inteligentes, o design adequado de sistemas de detecção de intrusão (IDS) é fundamental para proteger futuras infraestruturas de rede contra intrusos. Com o crescimento de coisas conectadas, os IDSs centralizados (baseados em nuvem) mais usados geralmente sofrem de alta latência e sobrecarga de rede, resultando em ataques sem resposta e detecção lenta de usuários mal-intencionados.

Neste artigo, aborda-se a limitação do IDS centralizado para dispositivos com recursos limitados, propondo dois métodos, semi-distribuídos e distribuídos, que combinam extração e seleção de recursos de bom desempenho e exploram análises coordenadas de ponta em neblina. Para distribuir as tarefas computacionais, desenvolvemos individualmente modelos paralelos de aprendizado de máquina correspondentes a um conjunto de dados de ataque particionado. No caso semi-distribuído, os modelos paralelos, executados no lado da borda, são aplicados para seleções de recursos lado a lado, que são seguidas por uma única classificação perceptron multicamada executada no lado do nevoeiro. No caso distribuído, os modelos paralelos realizam individualmente tanto a seleção de recursos quanto a classificação perceptron multicamada, após o que as saídas são combinadas por uma borda de coordenação ou névoa para a tomada de decisão final.

Com base no estudo comparativo de trabalhos existentes, os resultados numéricos demonstram a promessa dos métodos propostos, dando uma precisão de detecção comparável ao IDS centralizado superior, bem como exemplificam seus trade-offs inerentes entre a precisão e o desempenho do tempo de construção.

4. ASPECTOS RELEVANTES

Nos últimos anos, pesquisadores têm usado algoritmos CNN para realizar pesquisas de detecção de intrusão em vários campos, como Internet das Coisas, sistemas de controle industrial, sistemas de controle veículos autônomos e redes auto-organizadas em veículos e assim por diante, e obtiveram resultados relativamente bons. A CNN tem uma forte capacidade de reconhecimento principalmente porque sua camada de convolução tem uma forte capacidade de extrair recursos dos dados. Portanto, muitos estudiosos utilizam primeiro a CNN para extrair recursos dos dados e, em seguida, outros classificadores para tomar decisões quando houver melhorias na fusão de algoritmos. (ZHANG et al., 2022)

Atualmente, a IoT e seu significado tocaram todos os domínios. Além disso, sua segurança já havia atraído a atenção de um grande número de dispositivos e especialistas em rede. No entanto, sua implantação, uso e impacto na infraestrutura revelam muitos desafios e deficiências, abrindo caminho para novas áreas de pesquisa futuras. As raízes das preocupações com privacidade e segurança devem ser exploradas ainda mais para implantar infraestruturas de IoT de forma eficaz. O principal problema são os recursos restritos desses dispositivos, dificultando a adaptação de contramedidas avançadas atualmente implantadas em implantações de IoT (FAROOQ et al., 2022).

5. PROBLEMAS EXISTENTES

À medida que o acesso à Internet e as conexões aumentam, também aumentam os tipos de ataques cibernéticos. A análise de vários dados de detecção de intrusão comprova uma lacuna significativa no número de diferentes tipos de ataques, e o número de normais e anormais também é diferente. Portanto, os dados de detecção de intrusão têm um problema de desequilíbrio de dados. Esse problema é uma das razões essenciais pelas quais é difícil para os modelos de detecção de intrusão melhorarem seu desempenho (ZHANG et al., 2022).

Comparado com outros algoritmos de aprendizado de máquina, o CNN é mais difícil de alcançar o aprendizado incremental. A introdução de grandes quantidades de novos dados pode fazer com que a CNN sofra um esquecimento catastrófico. Alguns estudiosos melhoraram a estrutura (LI; HOIEM, 2018). Com base nessa rede, existem muitos métodos de treinamento diferentes para alcançar o aprendizado incremental. Mas esses métodos têm dificuldade em equilibrar as taxas de aprendizado do modelo para classes novas e antigas ou levam muito tempo para treinar com todos os dados. À medida que os tipos aumentam, a estrutura se torna mais proeminente e o treinamento se torna mais ineficiente, o que pode eventualmente fazer com que o sistema entre em colapso.

Os sistemas convencionais de detecção de intrusão de rede geralmente são pré-configurados para detectar ataques de rede mal-intencionados. Hoje, os invasores se aprofundaram e podem tentar contornar as regras comuns de detecção. Portanto, descobrir novos tipos de ataques tornou-se um dos pontos críticos e dificuldades em pesquisas futuras (ZHANG et al., 2022).

6. SOLUÇÕES POSSÍVEIS

Mulyanto et al. (2021) propõe um sistema de detecção de intrusão de rede baseado em perda focal, usando a função de perda focal para treinar o modelo CNN, reduzindo o peso de amostras fáceis de classificar, equilibrando as categorias de dados e melhorando efetivamente a taxa de detecção de amostras minoritárias. O modelo de detecção baseado na tecnologia de nivelamento de dados depende muito da capacidade de processamento de dados no estágio inicial. Em contraste, o modelo CNN processado por tecnologia algorítmica não requer pré-tratamento de dados balanceado, mas seu custo de tempo aumenta em comparação com o modelo de detecção de tecnologia em nível de dados. Ainda existem muitas soluções para o problema do desequilíbrio de dados, que precisam ser aprimoradas e inovadas por mais acadêmicos.

O modelo de detecção de intrusão baseado em uma rede neural convolucional multi-kernel proposto por Xiao et al. (2020) é um excelente método. O núcleo do algoritmo é oferecer unidades controladas na camada convolucional, que podem aprender novos dados com base na lembrança da categoria original. No entanto, este modelo ainda está em sintonia com a rede original, o que afetará a classificação da categoria original. Ao mesmo tempo,

para treinar melhor as novas categorias, o processamento de balanceamento de dados é necessário antes do treinamento do modelo.

6. PROJETO E DESENVOLVIMENTO DE UMA PROPOSTA

O trabalho de Mulyanto et al. (2021) comenta acerca de uma das problemáticas supramencionadas: o desequilíbrio de dados. O presente trabalho busca construir uma rede neural sensível ao custo baseada em perda focal, chamada de sistema de detecção de intrusão de rede de perda focal (FL-NIDS). É importante destacar que as subseções abaixo são todas resumos do trabalho de Mulyanto et al. (2021), sendo o presente artigo apenas uma tradução e resumo do trabalho construído.

6.1 METODOLOGIA

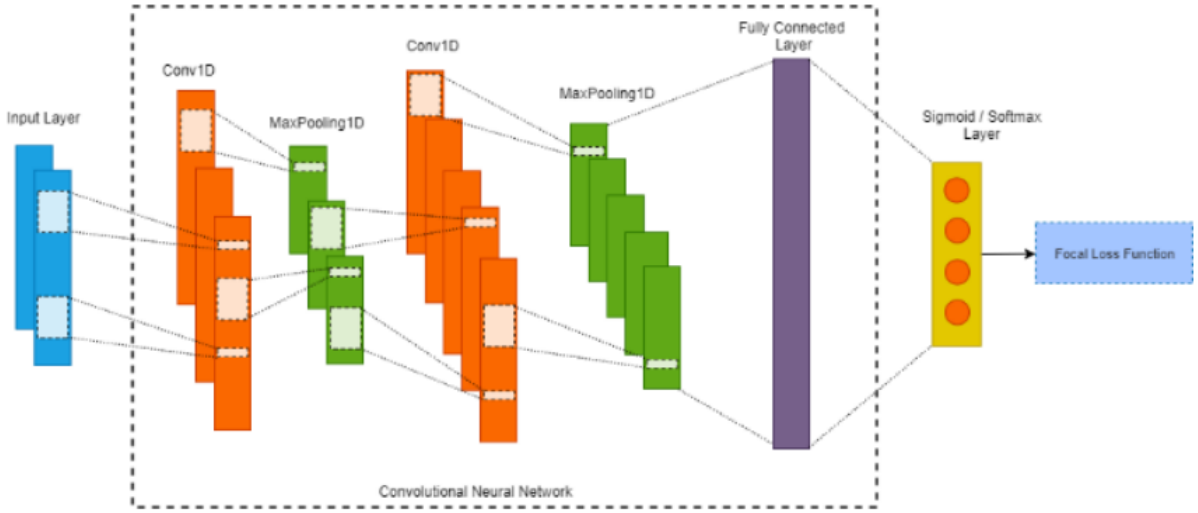
Mulyanto et al. (2021) utilizou a técnica de sobreamostragem, que compensa conjuntos de dados desequilibrados. Essa técnica concentra-se em modificar a classe minoritária (oversampling) e a classe majoritária (undersampling). A sobreamostragem refere-se à modificação da distribuição de dados para que a aparência das amostras seja baseada no custo calculado. Em outras palavras, essa técnica duplica dados de treinamento de custo mais alto até que a distribuição de dados seja proporcional a seus custos.

Uma rede neural profunda utiliza uma função de perda para otimizar os parâmetros. Normalmente, a função de perda atribui a entropia cruzada, que usa a função sigmóide para classificar a classe binária e a função softmax para conduzir a classificação multiclasse.

Neste artigo, os autores propõem o FL-NIDS, que pode ser aplicado em redes neurais profundas e redes neurais convolucionais, para superar o problema de NIDS desbalanceado. A perda focal foi utilizada como uma função de perda na saída da sub-rede de classificação. A arquitetura da rede neural profunda é mostrada na Figura 2, e a arquitetura da rede neural de convolução é mostrada na Figura 3. A rede neural profunda incluía três camadas: camada DNN 1, camada DNN 2 e camada DNN 3. Cada camada incluía uma camada densa seguida por uma camada dropout e uma camada softmax para classificação multiclasse e uma camada sigmóide para classificação binária.

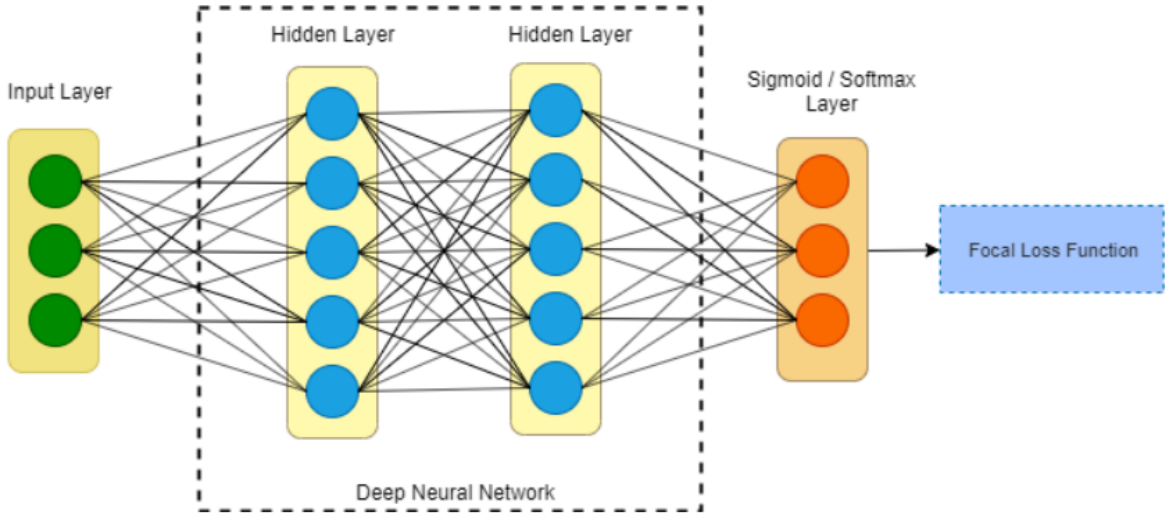
Outro algoritmo, CNN, foi introduzido com três camadas: CNN camada 1, CNN camada 2 e CNN camada 3. Cada camada incluía uma camada convolucional 1D com um tamanho de filtro de três. Cada duas camadas foram normalizadas usando 1D MaxPooling com um tamanho de filtro de dois, que foi seguido por uma camada de dropout com uma taxa de 0,2. O ajuste de hiperparâmetros foi utilizado usando um tamanho de lote de 64. O otimizador Adam com uma taxa de aprendizado de 0,0001 e decaimento de 0,004 foi usado. O treinamento incluiu 250 épocas com a opção de parar usando o parâmetro de parada antecipada de 25. Para mostrar a eficácia do FL-NIDS, vários algoritmos, como SMOTE, bem como CNN e DNN com entropia cruzada, foram comparados.

Figura 2 – Arquitetura da rede neural profunda



Fonte: Mulyanto et al. (2021).

Figura 3 – Arquitetura da rede neural de convolução



Fonte: Mulyanto et al. (2021).

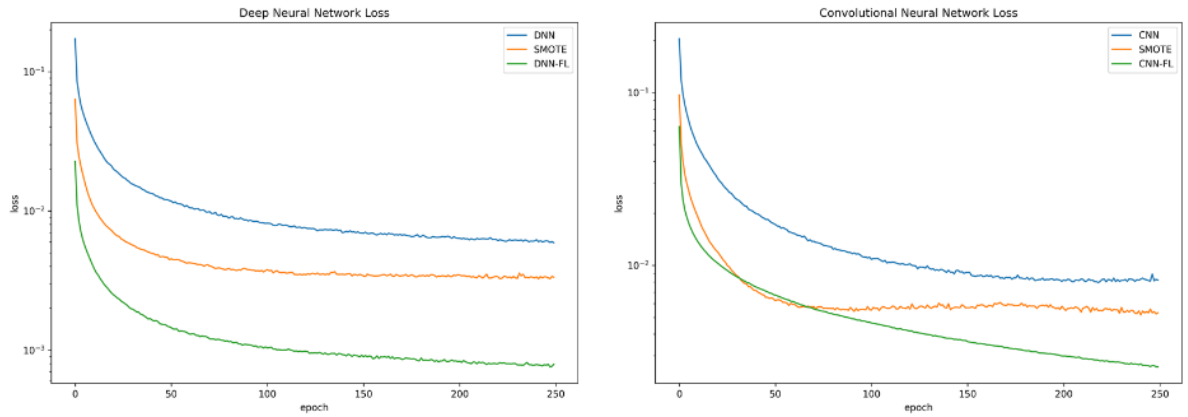
Os conjuntos de dados de referência para NIDS são atualmente limitados. A maioria deles são simulações de rede interna baseadas em simulações de tráfego e dados de ataque. Esta pesquisa utilizou três conjuntos de dados de referência para NIDS: NSL-KDD, UNSW-NB15 e Bot-IoT. Eles foram consistentemente utilizados para avaliar a eficácia dos algoritmos de aprendizado de máquina. NSL-KDD: Este conjunto de dados é a versão atualizada do KDDCup99 que remove os dados redundantes e registros inválidos. Essa versão limpa evita que o algoritmo de aprendizado de máquina seja influenciado durante a fase de dados de treinamento. O conjunto de dados normalmente inclui as informações de conexão com 41 recursos e seus rótulos associados, e há cinco categorias de rótulos: normal, DoS (negação de serviço), R2L (acesso não autorizado de uma máquina remota), U2R (acesso não autorizado a privilégios de raiz local) e sondagem (vigilância e outras sondagens). UNSW-NB15: Este

conjunto de dados é formado a partir de uma simulação de rede. A simulação é estabelecida criando uma rede que consiste em um servidor e um roteador. O servidor gera dados de tráfego simulados, incluindo tráfego de dados normal e dados maliciosos. O roteador captura os dados de tráfego simulados. O conjunto de dados consiste em 10 classes e 42 recursos. Bot-IoT: este novo conjunto de dados NIDS abrange todos os 11 ataques típicos atualizados, como DoS, negação de serviço distribuída (DDoS), reconhecimento e roubo. O Bot-IoT2019 contém um grande número de pacotes de tráfego e tipos de ataque que ocorreram durante cinco dias consecutivos. O conjunto de dados completo abrange 3.119.345 instâncias e 15 recursos contendo cinco rótulos de classe (um normal e quatro rótulos de ataque).

6.2 RESULTADOS E DISCUSSÃO

Neste experimento, foi comparada a entropia cruzada de DNN e CNN utilizando CE e SMOTE. A Figura 4 mostra a função de perda em comparação com DNN e a função de perda em comparação com CNN usando as respectivas técnicas. Ambos os modelos que utilizaram perda focal convergiram mais rapidamente em comparação com DNN CE, CNN CE, DNN SMOTE e CNN SMOTE. Além disso, o modelo proposto obteve erros de perda mínima que foram 7 vezes melhores para a arquitetura DNN e 3,7 vezes melhores para a arquitetura CNN do que o CNN SMOTE. Também teve melhor generalização, conforme mostrado pelas perdas de validação.

Figura 4 – Comparação da função de perda. (a) modelo de rede neural profunda (DNN). (b) modelo de rede neural convolucional (CNN).



Fonte: Mulyanto et al. (2021).

Em termos de precisão, o desempenho do FL-NIDS aplicando a arquitetura DNN e CNN foi comparável ao DNN CE, DNN SMOTE, CNN CE e CNN SMOTE. Os resultados mostraram que a acurácia foi igualmente distribuída, o que implica que as técnicas são comparáveis entre si. A distribuição de precisão dos conjuntos de dados NSL-KDD e UNSW-NB15 foi localizada em aproximadamente 77–89% na classificação binária e ligeiramente inferior em aproximadamente 66–78% na classificação multiclasse. O oposto ocorreu no conjunto de dados Bot-IoT. A distribuição de precisão foi localizada em aproximadamente 75-89% na

classificação binária e ligeiramente superior em aproximadamente 98-99% para a classificação multiclasse. Mais detalhadamente, na classificação binária e classificação multiclasse usando a arquitetura DNN, o FL-NIDS superou o DNN CE em no máximo 5% em três camadas usando o conjunto de dados Bot-IoT. No entanto, em alguns casos, o FL-NIDS também superou a precisão do DNN CE e do DNN SMOTE. Na arquitetura baseada em CNN, o FL-NIDS obteve precisão ainda melhor superando CNN CE e CNN SMOTE em no máximo 2%. Porém, em alguns casos, o FL-NISD também superou a acurácia de ambos. Este resultado indica que o FL-NIDS possui desempenho efetivo de classificação binária e multiclasse e é capaz de classificar potenciais ameaças futuras.

7. Conclusões

Neste trabalho foi realizada uma revisão do estado da arte em aperfeiçoamentos do gerenciamento de segurança de sistema de detecção de intrusão para Internet of Things com Fog Computing utilizando métodos de aprendizado de máquina supervisionada, onde foi possível elencar possíveis problemas e soluções, assim como uma proposta para parte dos problemas elencados, a abordagem de perda focal para classificação minoritária em sistemas de detecção de intrusão de rede por Mulyanto et al. (2021). O estudo explorou um método aprimorado de rede neural de entropia cruzada, denominado FL-NIDS, que pode ser aplicado à detecção de intrusão. A eficácia do algoritmo foi examinada usando três conjuntos de dados NIDS de referência que sofrem de classes desequilibradas. Os resultados mostraram que o FL-NIDS melhorou a precisão da detecção em conjuntos de dados desbalanceados em comparação com a arquitetura tradicional DNN e CNN. Esses resultados são consistentes com a hipótese de que a perda focal ajusta o peso de amostras preditas falsas. Como a detecção de intrusão é necessária para um ataque adversário, os autores sugerem aplicar a perda focal a outros conjuntos de dados, como tarefas sequenciais.

REFERÊNCIAS

AL-FUQAHA, A. et al. Internet of things: A survey on enabling technologies, protocols, and applications. **IEEE Communications Surveys Tutorials,** v. 17, n. 4, p. 2347–2376, 2015.

BONOMI, F. et al. Fog computing and its role in the internet of things. In: **Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing**. New York, NY, USA: Association for Computing Machinery, 2012. (MCC '12), p. 13–16. ISBN 9781450315197. Disponível em: https://doi.org/10.1145/2342509.2342513.

CHEN, Y. et al. Intrusion detection using multi-objective evolutionary convolutional neural network for internet of things in fog computing. **Knowledge-Based Systems**, v. 244, p. 108505, 2022. ISSN 0950-7051. Disponível em: https://www.sciencedirect.com/science/article/pii/S0950705122002179.

CONTI, M. et al. Internet of things security and forensics: Challenges and opportunities. **Future Generation Computer Systems**, v. 78, p. 544–546, 2018. ISSN 0167-739X. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167739X17316667.

FAROOQ, U. et al. Machine learning and the internet of things security: Solutions and open challenges. **Journal of Parallel and Distributed Computing**, v. 162, p. 89–104, 2022. ISSN 0743-7315. Disponível em:
https://www.sciencedirect.com/science/article/pii/S0743731522000235.

IORGA, M. et al. **Fog Computing Conceptual Model**. [S.l.]: Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2018.

LI, Z.; HOIEM, D. Learning without forgetting. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 40, n. 12, p. 2935–2947, 2018.

MULYANTO, M. et al. Effectiveness of focal loss for minority classification in network intrusion detection systems. **Symmetry**, v. 13, n. 1, 2021. ISSN 2073-8994. Disponível em: https://www.mdpi.com/2073-8994/13/1/4.

RAHMAN, M. A. et al. Scalable machine learning-based intrusion detection system for iot-enabled smart cities. **Sustainable Cities and Society**, v. 61, p. 102324, 2020. ISSN 2210-6707.
Disponível em: https://www.sciencedirect.com/science/article/pii/S221067072030545X.

XIAO, K. et al. Intrusion detection method based on incremental convolution neural network. **J. Comput. Appl.**, v. 40, p. 73 – 79, 2020.
Disponível em: https://www.scopus.com/inward/record.uri?eid=2-s2.0-

85104182744partnerID=40md5=9ce6b0b0f85d9667a0ed04006175d043.

ZHANG, C. et al. Comparative research on network intrusion detection methods based on machine learning. **Computers Security**, v. 121, p. 102861, 2022. ISSN 0167-4048. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404822002553.