Aprendizado Federado para Detecção de Ataques

Blenda Oliveira Mazetto[1], **Bruno Bogaz Zarpelão**[1]

[1]Departamento de Computação – Universidade Estadual de Londrina (UEL)
Caixa Postal 10.011 – CEP 86057-970 – Londrina – PR – Brasil

blenda.mazetto@uel.br, brunozarpelao@uel.br

Abstract. *In the last decades, the Internet has increasingly become an essential part of everyday life. As a consequence, network intrusions have became a big problem. In this case, Machine Learning (ML) techniques are playing a pivotal role in the early classification of the attacks in case of intrusion detection within the system, so it has been widely applied in Intrusion Detection Systems (IDS). However, the large amount of data required for training raises concerns about data privacy. Federated learning was created with the objective of solving this problem, it is a technique that can be performed collaboratively, and their main characteristic is the effort to avoid problems related to privacy. This project studies approaches for intrusion detection based on federated learning, intending an evaluation of results and comparison between techniques studied within this paradigm and a traditional machine learning approach.*

Resumo. *Nas últimas décadas, a Internet tornou-se cada vez mais uma parte essencial da vida cotidiana, graças a isso, as intrusões de rede se tornaram um grande problema. Neste caso, as técnicas de Aprendizado de Máquina (ML - Machine Learning) estão desempenhando um papel fundamental na classificação precoce dos ataques em caso de detecção de intrusão dentro do sistema, por isso tem sido amplamente aplicada em Sistemas de Detecção de Intrusão (IDS - Intrusion Detection Systems). No entanto, a grande quantidade de dados necessários para o treinamento levanta preocupações sobre a privacidade das informações utilizadas. O aprendizado federado foi criado com o objetivo de solucionar esse empecilho, é uma técnica que pode ser realizada de forma colaborativa, e sua principal característica é o esforço para evitar problemas relacionados à privacidade. Este trabalho propõe um estudo de abordagens baseadas em aprendizado federado, intencionando uma avaliação de resultados e comparação entre técnicas estudadas dentro deste paradigma e uma abordagem tradicional de aprendizado de máquina.*

1. Introdução

Com o desenvolvimento rápido da tecnologia, a internet se tornou parte diária da vida e uma ferramenta essencial. Como consequência, as intrusões em redes comerciais e privadas tem sido motivo de preocupação. O aprendizado de máquina vem sendo amplamente utilizado para a detecção de intrusão, pois permite criar sistemas mais facilmente adaptáveis a diferentes realidades e contextos. São diversas as técnicas existentes utilizadas nos sistemas de detecção de intrusão [29].

O uso do aprendizado de máquina pode levantar questões sobre a privacidade das informações usadas em seu treinamento, especialmente por conta da demanda de

grandes volumes de dados. Em 2018, foi revelado que o Facebook treinou um modelo de detecção de objetos usando 3.5 bilhões de imagens vindas do Instagram. O modelo treinado superou os outros modelos existentes demonstrando a importância da quantidade de dados [11]. Esse evento fez com que a privacidade fosse novamente uma preocupação na mente dos usuários da internet, motivando a busca por técnicas de aprendizado de máquina que tenham como característica a preservação de privacidade.

Para detectar ataques em redes e sistemas de computadores, os IDSs precisam coletar, armazenar e analisar uma ampla gama de dados. Esses dados podem conter informações privadas e, portanto, a operação de um IDS pode ter consequências relacionadas à privacidade [20].

O Aprendizado Federado (FL - Federated Learning) [31], traz a possibilidade de um treinamento descentralizado, onde os dados locais são privados e o objeto compartilhado é um modelo de aprendizado. Nessa abordagem, cada um dos participantes do treinamento começa com um modelo genérico inicial fornecido pelo servidor central seguro. Com seus dados locais, cada participante realiza o treinamento do modelo recebido, e após a etapa de treinamento cada um dos participantes envia seu modelo treinado, para o servidor central. Após isso, o servidor agrega esses modelos gerando um novo modelo de rede neural. O modelo agregado é enviado para os participantes repetindo as etapas citadas anteriormente até que o treinamento esteja completo.

A literatura apresenta diferentes técnicas usando o aprendizado federado [8, 4, 34, 30, 9]. Em [23] e [33] é explorado o aprendizado não supervisionado. Mesmo tendo como prioridade a segurança das informações, o aprendizado federado também está exposto a ataques maliciosos [16], tendo isso em vista, [27] e [14] trazem métodos para melhorar seus sistemas e proteger os dados usados no treinamento das redes neurais. Algumas técnicas consistem em fazer modelos que agrupem as amostras mais parecidas em grupos como clusters [7], ou então segmentar esses grupos fazendo com que cada um tenha seu próprio modelo de rede neural [26, 28].

No campo de Internet da Coisas (IoT - Internet of Things), o FL vem ganhando importância com diversos trabalhos já utilizando este paradigma para sistemas de segurança [19]. Em [24] existe uma investigação das possibilidades trazidas pelo aprendizado federado em relação à detecção de malwares em IoT, além de um estudo de questões de segurança inerentes a esse novo paradigma de aprendizado.

Neste projeto, será estudado o uso do aprendizado federado para a detecção de intrusão preservando a privacidade dos dados. Inicialmente será feita uma pesquisa dentro da literatura existente, seguida de uma seleção de métodos que utilizam o paradigma. Os métodos selecionados serão estudados mais profundamente, avaliando a possibilidade de implementação e sua eficiência como IDS. Os métodos implementados serão comparados com o aprendizado de máquina tradicional e os resultados sintetizados em uma tabela, algumas métricas a serem avaliados são: F1-score, precisão, recall, acurácia, positivo verdadeiro, falso positivo, negativo verdadeiro e falso negativo. Para o treinamento e realização dos experimentos serão utilizados conjuntos de dados publicamente disponíveis para detecção de intrusão.

2. Fundamentação Teórico-Metodológica e Estado da Arte

2.1. Aprendizado de Máquina

Aprendizado de máquina é um ramo da inteligência artificial (IA) e da ciência da computação projetado para emular a inteligência humana aprendendo com o ambiente ao redor por meio da experiência [17].

Por meio do uso de métodos estatísticos, os algoritmos são treinados para fazer classificações ou previsões. Essas previsões subsequentemente conduzem a tomada de decisões [2]. Esses algoritmos recebem os dados que devem ser avaliados, esses, podem estar presentes em um banco de dados, por exemplo. A maquina então analisa as informações recebidas, e com o uso de propriedades estatísticas, entrega uma resposta de acordo com o problema proposto. O método de aprendizado pode ser classificado em supervisionado, não supervisionado, e semi supervisionado [13].

O aprendizado não supervisionado possui dados não rotulados que o algoritmo deve tentar identificar semelhanças e reagir conforme a presença ou ausência de tais semelhanças em cada novo dado. Nesse cenário, o algoritmo vai encontrar padrões para agrupar (ou clusterizar) as amostras semelhantes. Enquanto o aprendizado supervisionado, tem os conjuntos de dados rotulados para que o modelo aprenda a partir de resultados pré definidos. Na prática, esse tipo de aprendizado depende da intervenção humana, nesses modelos é possível dar pesos ou calibrar o nível de assertividade e de precisão de um modelo. Por fim, o método semi-supervisionado combinam os dois anteriores. Parte dos testes acompanham um rótulo de saída e parte não.

2.2. Sistemas de Detecção de Intrusão

Um Sistema de Detecção de Intrusão é software que tem como função monitorar diferentes parâmetros de funcionamento do sistema que visa proteger a fim de encontrar eventos que possam violar suas regras de segurança. O IDS pode escolher diferentes abordagens em relação a seu posicionamento e ao seu método de detecção [18].

Um sistema NIDS (Network Intrusion Detection Systems) foca em analisar o fluxo de informações que transitam pela rede, buscando encontrar padrões comportamentais suspeitos. Neste sistema a IDS é geralmente posicionada em locais estratégicos da rede. Nessa analise o IDS verifica os pacotes capturados em busca de tentativas de invasão, além de comportamentos de uma rede comprometida [32].

Por outro lado, um sistemas HIDS (Host-based Intrusion Detection Systems) foca em examinar ações específicas com base nos hospedeiros, como por exemplo os arquivos que são acessados, aplicativos utilizados, ou informações de logs. Nesta, a IDS está presente em todos os hospedeiros, sendo cada um responsável pelo próprio comportamento. Para a verificação, são avaliados o uso de CPU, memória, energia, conexões na rede, portas usadas, números de tarefas sendo executadas, entre outros [32]. Quanto a estratégia de detecção, os IDSs podem ser implementados de duas formas. O primeira método é a detecção por assinatura (Signature-Based IDS), no qual o sistema deve conhecer previamente os padrões utilizados em cada tipo de ataque que ele poderá identificar. Esta estratégia permite a rápida identificação de ataques conhecido. Por outro lado, ataque que não tenham padrões similares a algum conhecido podem se passar como um trafego normal [12, 21].

A segunda abordagem é a detecção por anomalia (Anomaly-Based IDS). Neste método o sistema busca por ações ou comportamentos que fogem do padrão no dispositivo ou tráfego de rede. Quando um comportamento que difere desses padrões ocorre, ele é catalogado como anômalo. Esta estratégia não necessita que o sistema conheça previamente os padrões dos ataques, porém pode gerar uma quantidade considerável de falsos positivos [6, 21].

Muitos sistemas de detecção de intrusão ainda sofrem com uma alta taxa de falsos alarmes, gerando muitos alertas para situações pouco ameaçadoras, o que aumenta a carga dos analistas de segurança e pode fazer com que ataques seriamente prejudiciais sejam ignorados. Assim, muitos pesquisadores têm se concentrado no desenvolvimento de IDSs com taxas de detecção mais altas e taxas de alarmes falsos reduzidas. Outro problema com os IDSs existentes é que eles não têm a capacidade de detectar ataques desconhecidos. Como os ambientes de rede mudam rapidamente, variantes de ataque e novos ataques surgem constantemente. Assim, é necessário desenvolver IDSs que possam detectar ataques desconhecidos.

Para resolver os problemas acima, os pesquisadores começaram a se concentrar na construção de IDSs usando métodos de aprendizado de máquina [15].

2.3. Aprendizado Federado

Durante um processo de treinamento, é necessário uma grande quantidade de dados, se tratando de um sistema de detecção de intrusão, existe a necessidade de coletar, armazenar e analisar um amplo volume deles. Esses dados referentes a usuários e organizações podem conter informações privadas que o provedor não gostaria de compartilhar, levantando preocupações em relação a privacidade.

O aprendizado federado permite realizar aprendizado de máquina de forma colaborativa, com um modelo de previsão compartilhado, mantendo todos os dados de treinamento no dispositivo. Seu funcionamento pode ser descrito em algumas etapas.

1. Os dispositivos participantes do treinamento recebem o modelo.
2. Cada participante treina o seu modelo recebido com seus dados locais
3. Todos os dispositivos enviam o modelo treinado para o servidor central.
4. O servidor central agrega os modelos recebidos em único modelo
5. O servidor central envia o modelo agregado para todos os dispositivos participantes

Todos os dados de treino permanecem nos dispositivos locais e nenhuma atualização individual é armazenada no servidor [1].

Dentro do FL, diferentes abordagens podem ser executadas. Em [23] e [33] o método de aprendizado não supervisionado é explorado, sendo que em [23] a rede neural é um autoencoder, enquanto [33] utiliza uma Multitask Deep Neural Network como classificador.

Sistemas que utilizam FL se deparam com alguns desafios [3], um deles é a engenharia reversa que pode ser feita em modelos de redes neurais por ataques [16]. Tendo como objetivo melhorar a segurança nos sistemas que aplicam o aprendizado federado, [27] propõe o uso de blockchain para tornar o sistema inerentemente mais seguro.

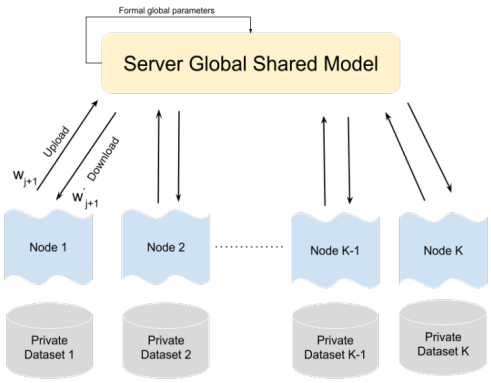

Figura 1. Diagrama de blocos Aprendizado Federado.

Outra abordagem possível de utilização é a aprendizado federado segmentado, ela consiste em acrescentar uma etapa de verificação, após N iterações, é feita uma comparação do modelo gerado a partir dos dados de treinamento do participante com o modelo agregado. Isso permite uma métrica do quanto o participante que está sendo avaliado está fora da média dos outros participantes. Se o participante avaliado exceder a limiar estipulada, é criado um novo modelo global ao qual ele vai pertencer [28] [26].

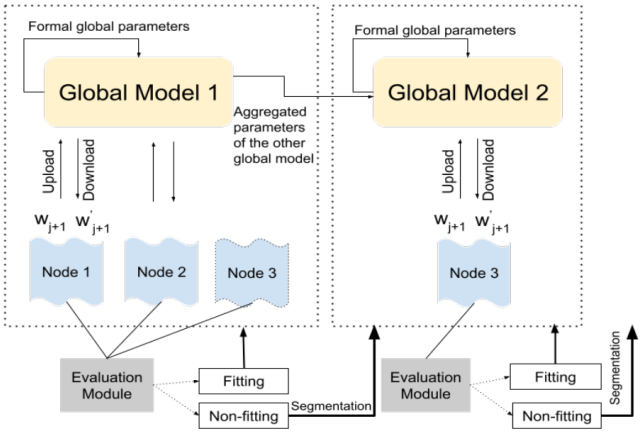

Figura 2. Diagrama de blocos Aprendizado Federado Segmentado.

3. Objetivos

Em trabalhos recentes, é possível ver o aprendizado federado sendo usado para formular a detecção de intrusão em um aprendizado semi-supervisionado onde tanto o aprendizado supervisionado (usando dados rotulados) quanto o aprendizado não supervisionado (sem dados rotulados) são combinados de forma colaborativa [5].

O aprendizado federado também entra na tentativa de superar desafios sobre o uso de dados para melhorar a segurança dos sistemas IoT, usando inteligência artificial, levando em consideração as limitações de recursos em dispositivos IoT e questões relacionadas à privacidade de dados [22, 25, 10].

O projeto tem como objetivo principal estudar diferentes técnicas de aprendizado de máquina aplicadas a sistemas de detecção de intrusão e fazer uma comparação entre elas, tendo como foco o estudo de métodos dentro de aprendizado federado. Os seguintes objetivos específicos foram definidos:

1. Realizar uma revisão bibliográfica dos trabalhos envolvendo técnicas de aprendizado federado para detecção de intrusão
2. Identificar técnicas de aprendizado federado que podem ser adequadas à aplicação em sistemas de detecção de intrusão.
3. Fazer um levantamento sobre conjuntos de dados disponibilizados publicamente que possibilitem a pesquisa com aprendizado federado.
4. Comparar as diferentes arquiteturas propostas comparando as vantagens e desvantagens de cada uma, inclusive com a aprendizado de máquina tradicional.

4. Procedimentos metodológicos/Métodos e técnicas

O primeiro passo será realizar uma revisão bibliográfica com o foco em encontrar técnicas do aprendizado federado que possam ser aplicadas em sistemas de detecção de intrusão. Essa revisão será feita com o objetivo de selecionar trabalhos que tenham uma possibilidade de replicação ou refatoração e que sejam interessantes para o projeto. Dentro das possibilidades, serão avaliados fatores como foco em preservação de privacidade, precisão, conjuntos de dados utilizados e resultados em geral.

Antes de partir para a implementação é necessário avaliar os conjuntos de dados possíveis de se trabalhar. A pesquisa de conjuntos de dados pode levar em consideração os exemplos encontrados durante a revisão bibliográfica mas não está restrito a isso. Os conjuntos de dados selecionados devem conter dados de tráfegos em redes, contendo amostras de ataques e naturais permitindo a emulação de situações onde a coleta de dados foi realizada de maneira distribuída.

Com as técnicas de aprendizado federado e os conjuntos de dados escolhidos, o próximo passo é realizar a implementação dos algoritmos utilizados nessas técnicas. Implementando, assim, sistemas de detecção de intrusão que utilizam aprendizado federado em seu desenvolvimento. Durante esse passo, caso algum modelo com rede neural seja escolhido, é importante testar múltiplos arquiteturas de redes neurais até encontrar a que melhor satisfaça o quesito de precisão.

Para as necessidades de aprendizado de máquina será feita uma busca por bibliotecas que facilitem a implementação de soluções de aprendizado federado como o PySyft.

A próxima etapa se resume em realizar diversas execuções fazendo testes com o objetivo de encontrar as configurações que trazem um melhor resultado.

Com os resultados dos testes em mãos, será apresentada uma comparação entre as técnicas escolhidas, os parâmetros avaliados serão acurácia, precisão, função de perda, quantidade de positivos verdadeiros, falsos positivos, negativos verdadeiros, falsos negativos e por último o calculo da F1-score.

5. Cronograma de Execução

Atividades a serem realizadas:

1. Revisão bibliográfica focada em técnicas de aprendizado federado;
2. Escolha dos conjuntos de dados;
3. Desenvolvimento de programas menores necessários para a utilização dos conjuntos de dados, divisão entre treinamento e teste;
4. Implementação das técnicas de aprendizado federado escolhidas anteriormente.
5. Realização de testes para encontrar a melhor arquitetura de rede neural (caso haja a implementação de uma rede neural);
6. Realização de testes para encontrar as melhores configurações dentro dos algoritmos;
7. Comparação entre as técnicas implementadas.

Tabela 1. Cronograma de Execução

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

6. Contribuições e/ou Resultados esperados

O principal resultado esperado deste projeto é poder identificar técnicas de preservação de privacidade que atendam sistemas de detecção de intrusão e realizar uma comparação entre elas. Ainda, espera-se entender os impactos e a eficácia do aprendizado federado nos sistemas de detecção de intrusão. Desta forma, este projeto permitirá melhor avaliação sobre a viabilidade da aplicação desses mecanismos de preservação de privacidade no contexto estudado.

7. Espaço para assinaturas

Londrina, *12 de setembro de 2022*.

Blenda Oliveira Mozetto

Aluno

Orientador

Referências

[1] Federated learning: Collaborative machine learning without centralized training data. https://ai.googleblog.com/2017/04/federated-learning-collaborative.html. Accessed: 2022-13-08.

[2] O que é machine learning? https://www.ibm.com/br-pt/cloud/learn/machine-learning. Accessed: 2022-13-08.

[3] Shaashwat Agrawal, Sagnik Sarkar, Ons Aouedi, Gokul Yenduri, Kandaraj Piamrat, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu. Federated learning for intrusion detection system: Concepts, challenges and future directions, 2021.

[4] Noor Ali Al-Athba Al-Marri, Bekir S. Ciftler, and Mohamed M. Abdallah. Federated mimic learning for privacy preserving intrusion detection. In *2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pages 1–6, 2020.

[5] Ons Aouedi, Kandaraj Piamrat, Guillaume Muller, and Kamal Singh. Fluids: Federated learning with semi-supervised approach for intrusion detection system. In *2022 IEEE 19th Annual Consumer Communications Networking Conference (CCNC)*, pages 523–524, 2022.

[6] Vitor Hugo Bezerra, Victor Guilherme Turrisi da Costa, Sylvio Barbon Junior, Rodrigo Sanches Miani, and Bruno Bogaz Zarpelão. Iotds: A one-class classification approach to detect botnets in internet of things devices. *Sensors*, 19(14):3188, 2019.

[7] Christopher Briggs, Zhong Fan, and Peter Andras. Federated learning with hierarchical clustering of local updates to improve training on non-iid data. In *2020 International Joint Conference on Neural Networks (IJCNN)*, pages 1–9, 2020.

[8] Zhuo Chen, Na Lv, Pengfei Liu, Yu Fang, Kun Chen, and Wu Pan. Intrusion detection for wireless edge networks based on federated learning. *IEEE Access*, 8:217463–217472, 2020.

[9] Gustavo de Carvalho Bertoli, Lourenço Alves Pereira Júnior, and Osamu Saotome. Improving detection of scanning attacks on heterogeneous networks with federated learning. 49(4):118–123, jun 2022.

[10] Phan The Duy, Tran Van Hung, Nguyen Hong Ha, Hien Do Hoang, and Van-Hau Pham. Federated learning-based intrusion detection in sdn-enabled iiot networks. In *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, pages 424–429, 2021.

[11] Florian Hartmann. Federated learning. *línea]. Available: https://florian. github. io/federated-learning/.[Último acceso: 15 10 2019]*, 2018.

[12] Ahmad Javaid, Quamar Niyaz, Weiqing Sun, and Mansoor Alam. A deep learning approach for network intrusion detection system. *Eai Endorsed Transactions on Security and Safety*, 3(9):e2, 2016.

[13] S.B. Kotsiantis, I.D. Zaharakis, and Pintelas. Machine learning: a review of classification and combining techniques. *Artif Intell Rev*, 26(1):159–190, 2006.

[14] Beibei Li, Yuhao Wu, Jiarui Song, Rongxing Lu, Tao Li, and Liang Zhao. Deepfed: Federated deep learning for intrusion detection in industrial cyber–physical systems. *IEEE Transactions on Industrial Informatics*, 17(8):5615–5624, 2021.

[15] Hongyu Liu and Bo Lang. Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences*, 9(20), 2019.

[16] Yuntao Liu, Dana Dachman-Soled, and Ankur Srivastava. Mitigating reverse engineering attacks on deep neural networks. In *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 657–662, 2019.

[17] T Mitchell, B Buchanan, G DeJong, T Dietterich, P Rosenbloom, and A Waibel. Machine learning. *Annual Review of Computer Science*, 4(1):417–433, 1990.

[18] Emilio Tissato Nakamura and Paulo L'ıcio de Geus. *Segurança de redes em ambientes cooperativos*. Novatec Editora, 2007.

[19] Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N. Asokan, and Ahmad-Reza Sadeghi. DÏot: A federated self-learning anomaly detection system for iot. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pages 756–767, 2019.

[20] Salman Niksefat, Parisa Kaghazgaran, and Babak Sadeghiyan. Privacy issues in intrusion detection systems: A taxonomy, survey and future directions. *Computer Science Review*, 25, 08 2017.

[21] 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.

[22] Safa Otoum, Nadra Guizani, and Hussein Mouftah. Federated reinforcement learning-supported ids for iot-steered healthcare systems. In *ICC 2021 - IEEE International Conference on Communications*, pages 1–6, 2021.

[23] D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen, and E. Ilie-Zudor. Chained anomaly detection models for federated learning: An intrusion detection case study. *Applied Sciences*, 2018.

[24] Valerian Rey, Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, and Gérôme Bovet. Federated learning for malware detection in iot devices. *Computer Networks*, 204:108693, 2022.

[25] Hassan Saadat, Abdulla Aboumadi, Amr Mohamed, Aiman Erbad, and Mohsen Guizani. Hierarchical federated learning for collaborative ids in iot applications. In *2021 10th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–6, 2021.

[26] Geet Shingi, Harsh Saglani, and Preeti Jain. Segmented federated learning for adaptive intrusion detection system, 2021.

[27] Andrew Ronald Short, Helen C. Leligou, Michael Papoutsidakis, and Efstathios Theocharis. Using blockchain technologies to improve security in federated learning systems. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 1183–1188, 2020.

[28] Yuwei Sun, Hiroshi Esaki, and Hideya Ochiai. Adaptive intrusion detection in the networking of large-scale lans with segmented federated learning. *IEEE Open Journal of the Communications Society*, 2:102–112, 2021.

[29] Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin, and Wei-Yang Lin. Intrusion detection by machine learning: A review. *Expert Systems with Applications*, 36(10):11994–12000, 2009.

[30] Hao Wang, Zakhary Kaplan, Di Niu, and Baochun Li. Optimizing federated learning on non-iid data with reinforcement learning. In *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, pages 1698–1707, 2020.

[31] Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, and H. Yu. Federated learning. *Morgan and Claypool*, 2019.

[32] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications*, 84:25–37, 2017.

[33] Ying Zhao, Junjun Chen, Di Wu, Jian Teng, and Shui Yu. Multi-task network anomaly detection using federated learning. SoICT 2019, page 273–279, New York, NY, USA, 2019. Association for Computing Machinery.

[34] Hangyu Zhu and Yaochu Jin. Multi-objective evolutionary federated learning. *IEEE Transactions on Neural Networks and Learning Systems*, 31(4):1310–1322, 2020.