SoK: federated learning based network intrusion detection in 5G: context, state of the art and challenges

Sara Chennoufi, Gregory Blanc, Houda Jmila, Christophe Kiennert

SoK: Federated Learning based Network Intrusion Detection in 5G: Context, State of the Art and Challenges

Sara Chennoufi
sara.chennoufi@telecom-sudparis.eu
Télécom SudParis, Institut Polytechnique de Paris
Palaiseau, France

Gregory Blanc
gregory.blanc@telecom-sudparis.eu
Télécom SudParis, Institut Polytechnique de Paris
Palaiseau, France

Houda Jmila
houda.jmila@cea.fr
Institute LIST, CEA, Paris-Saclay University
Palaiseau, France

Christophe Kiennert
christophe.kiennert@telecom-sudparis.eu
Télécom SudParis, Institut Polytechnique de Paris
Palaiseau, France

ABSTRACT

5G brings significant advancement, offering lower latency, and improved connectivity. Yet, its complexity, stemming from factors such as integrating advanced technologies like Software Defined Networking (SDN) and slicing, introduces challenges in implementing strong security measures against emerging threats. Although Intrusion Detection Systems (IDSs) can successfully detect attacks, the novelty of 5G creates an expanded attack surface. Collaboration is essential for detecting novel, distributed attacks, and ensuring comprehensive observability in multiparty networks. However, such collaboration raises privacy concerns due to the sensitivity of shared data. Federated Learning (FL), a collaborative Machine Learning (ML) approach, is a promising solution to preserve privacy as the model is trained locally without exchanging raw data.

In this paper, we examine ongoing efforts on FL-based IDS solutions in 5G. We set out to systematically review them in the light of challenges raised by their practical deployment in 5G networks. Out of the numerous papers we analyzed in FL, only 17 specifically concentrate on 5G scenarios making them the focus of this study. Towards systematizing knowledge, we first identify IDS challenges in 5G. Second, we classify FL-based IDS according to (i) their 5G application domain, (ii) 5G challenges they address, and (iii) their FL approach in terms of architecture, parameters, detection method, evaluation, etc. Through this examination, we find out that some issues receive less attention, prompting us to explore potential solutions. Additionally, we have identified other challenges, like the lack of evaluation results applicability due to the difficulties in getting high quality 5G datasets for evaluation.

CCS CONCEPTS

• **Security and privacy → Artificial immune systems**.

ARES 2024, July 30-August 2, 2024, Vienna, Austria

ACM ISBN 979-8-4007-1718-5/24/07.
https://doi.org/10.1145/3664476.3664500

KEYWORDS

5G, intrusion detection system, machine learning, network security, federated learning, privacy, heterogeneity.

ACM Reference Format:
Sara Chennoufi, Gregory Blanc, Houda Jmila, and Christophe Kiennert. 2024. SoK: Federated Learning based Network Intrusion Detection in 5G: Context, State of the Art and Challenges. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30-August 2, 2024, Vienna, Austria.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3664476.3664500

1 INTRODUCTION AND MOTIVATION

The dawn of 5G technology marks a transformative era in connectivity, promising unprecedented speeds, minimal latency, and the ability to support various interconnected devices. A set of technologies like *Software-Defined Networking*, *Network Function Virtualization* (NFV), and network slicing enables this. Yet, with innovation comes responsibility, and the security implications of 5G have become a central focus for researchers [45, 62].

Intrusion Detection Systems, effective in detecting attacks, may face new challenges with the expanded attack surface of 5G [1, 57]. Collaborative efforts become indispensable for ensuring knowledge sharing, enhancing the detection capabilities of new attacks, and reducing false positives.

However, integrating collaboration and distribution in intrusion detection may introduce privacy concerns, particularly in sensitive 5G applications like medical use cases. Therefore, *Federated Learning* (FL) emerges as the most promising candidate for developing *collaborative, distributed, and privacy-preserving* solutions for 5G IDS, given its inherent properties [58]. It constructs a global model from local client models trained on devices containing private data. Only the training results, like the trained models, gradients, or weights, are sent to the central server, reinforcing privacy. Besides, FL allows devices to train on their own data, reducing the load on the central server and minimizing network charges by transmitting only models, not data.

While FL is increasingly adopted, its application in 5G networks presents challenges and concerns. We outline five specific challenges. *First*, with the proliferation of connected devices and diverse applications, *5G networks generate large amounts of data, at high transmission rates* [41, 67], underscoring the importance of scalability in deploying IDS. The high data rates of 5G networks

present a challenge for real-time intrusion detection. *Second, 5G networks are heterogeneous* [7]. *Data structure heterogeneity* in 5G refers to the varied formats and characteristics of data like voice, text, and IoT sensor data. IDS must employ adaptable algorithms to analyze diverse traffic effectively. *Behavior heterogeneity* considers the challenge of diverse behaviors exhibited by components in 5G networks, causing difficulties in establishing a static baseline for normalcy, requiring adapted intrusion detection methods to handle the evolving network dynamics. In ML, this is also known as *concept drift. Third, certain 5G devices have limited resources*, such as IoT devices [53], which may be insufficient for training models. Then, some IoT devices with limited batteries are event-driven, so they are only on when an event occurs. This challenges IDS development due to unpredictable event occurrences. Besides, heterogeneous device resource constraints affect collaborative IDS design since they pose synchronization issues. *Fourth, 5G networks handle high mobility and support virtualization* [41]. High mobility challenges the deployment of IDS due to changing traffic patterns and user dynamics, while virtualization limits IDS observability. These challenges also make continuous threat detection difficult for IDS. *Finally, 5G should preserve privacy in multi-party networks* where different entities have varying access and control. Achieving comprehensive observability for IDS requires collaboration. In such cases, IDS must follow data privacy regulations and leverage privacy-preserving techniques, which could limit their intrusion detection capabilities.

In this paper, we first study and classify state-of-the-art solutions based on i) the targeted 5G application domain, ii) their alignment with the above 5G characteristics, and iii) the used FL approach. Then, we identify gaps in addressing these challenges. We delve into potential solutions that researchers and industry professionals can employ to tailor FL-based IDS to suit their 5G scenarios.

The use of FL in IDSs has been explored by several surveys. Lavaur et al. [50] proposed a reference architecture and developed a taxonomy to categorize FL IDS systems based on various federation settings. Another survey [5] investigated the challenges and potential future directions of FL based IDS. In particular, the utilization of blockchain-based network transactions to ensure secure transaction records. Fedorchenko et al. [32] analyzed FL based IDS architecture, examined them in various application domains, and compared them. The utilization of FL based IDS for IoT was investigated by several authors [8, 12, 14, 21]. However, none of these studies have specifically addressed the unique requirements and challenges of implementing IDSs in 5G networks. Issues such as handling the massive volume of data, ensuring real-time detection, and adapting to virtualization and dynamism in 5G environments require specialized approaches. To our knowledge, this is the *first Systematization of Knowledge* (SoK) paper in this field. It aims to answer the following research questions: **RQ1.** What characteristics of 5G pose challenges for IDS design? **RQ2.** How have these challenges been addressed by 5G use cases, and which variants of FL-based IDS have been used? **RQ3.** How can 5G-related challenges for FL-based IDS be addressed, and what are the future directions in this area?

The key contributions of this paper can be summarized as follows:

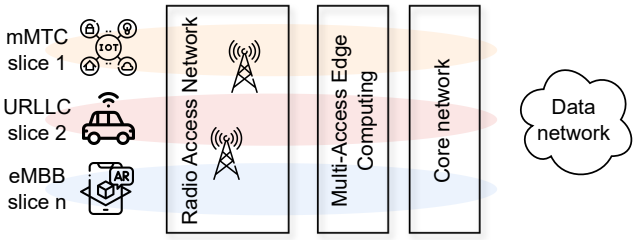

Figure 1: Simplified 5G architecture

- we motivate collaborative approach for intrusion detection, with a primary focus on FL-based IDS in the context of 5G networks;
- we identify specific 5G network characteristics and elucidate the requirements they impose on the design of IDS;
- we conduct an examination and classification of the current FL-based IDS in 5G networks, analyzing their application across various use cases. Additionally, we evaluate their alignment with 5G characteristics, scrutinize the FL parameters, and analyze the detection method and evaluation employed;
- we explore challenges associated with meeting the identified requirements, present potential solutions, and highlight opportunities arising from addressing these challenges.

To perform this SoK, we collected papers from academic sites such as Google Scholar. We focused on articles about 5G FL-based intrusion detection. To refine the search results, we only included the most relevant papers. We identified a sample of 17 papers that held sufficient significance to perform our analysis.

This paper is organized as follows: Section 2 introduces the necessary background on FL and 5G, including the FL framework, and parameters as well as 5G use case classes, architecture, and enabling technologies. Subsequently, Section 3 analyzes the retained FL-based IDS and classifies them to outline the current state of the art. Finally, Section 4 delves into the challenges that 5G poses for FL-based IDS and provides potential solutions.

2 BACKGROUND

2.1 5G architecture, use cases, and enablers

5G architecture as shown in Fig. 1 includes the following components: *User Equipment* (UE) for end-users; *Core Network* (CN), i.e., the main backbone providing various network functions; *Radio Access Network* (RAN) which connects wireless devices to the core; and *Management and Orchestration* (MANO) which ensures efficient network service deployment.

5G aims to include a variety of use cases classified by The International Telecommunication Union Radiocommunication Sector (ITU-R) [2] into three classes: *Enhanced Mobile Broadband* (eMBB) which focuses on delivering high data rates and improved network capacity to support applications like ultra-HD video streaming; *Ultra-Reliable Low Latency Communications* (URLLC) which emphasizes real-time and mission-critical services like autonomous vehicles; and *Massive Machine Type Communications* (mMTC) for massive device connectivity like IoT.

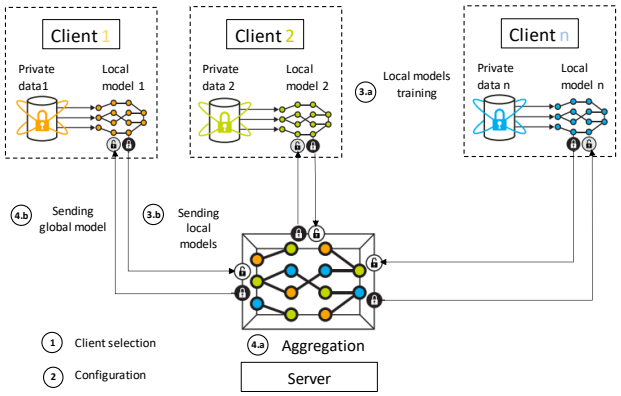

Figure 2: Federated Learning process

To enhance performance and facilitate connectivity for various applications within a unified network, 5G uses enabling technologies like NFV, network slicing for customized networks, *Multi-Access Edge Computing* (MEC) for localized computation, and SDN for dynamic management.

2.2 Federated Learning

The *FL architecture*, as depicted in Figure 2, comprises N clients with private data and a central server managing and coordinating training. Clients can be individuals, companies, hospitals, etc. Depending on the *client type*, FL can be classified into *cross-silo*, which includes a small number of clients with powerful resources like ISPs and companies, and *cross-device*, which involves a larger number of participants with limited resources and computing power, like IoT or other UE devices. Other variants of FL architecture exist, like *hierarchical* – with multiple levels of aggregation – and *decentralized*. A *decentralized* FL does not rely on a central server, and clients communicate directly with each other, often through peer-to-peer communication. This approach can prevent the occurrence of a *Single Point of Failure* (SPoF). Clients are *incentivized* to participate in the FL process to either benefit from the resultant model enhancements or gain financial rewards. Management of this participation can be facilitated through contractual agreements or other methodologies, like the application of game theory [42].

The *FL process* is articulated around four phases. *First*, in the *client selection* phase, a large number of devices announce their availability to participate, and a limited number are selected by the central server based on certain criteria, such as the optimal number of clients [17]. *Second*, in the *configuration* phase, the server sends the FL plan that contains information on the execution method and initialization for the ML model to the selected devices. *Third*, in the *local training* phase, the selected devices train a local ML model on their data and send it to the server. Initially, they *preprocess* their data by conducting tasks like feature extraction, feature selection, and dimensionality reduction if needed. Then, they *train a local ML model* on this local data. This model can be supervised if data are labeled, unsupervised if data are unlabeled, or semi-supervised when combining both. *Local training location* can be either on the client's device – when it bears sufficient resources – or at another location such as a *gateway* or the MEC – when resources are limited, e.g., IoT devices [50, 82]. *Fourth*, in the *aggregation* phase, the server executes the *aggregation algorithm* that takes as input clients' local models and returns a *global model*. The basic aggregation algorithm is *Federated Averaging* (FedAvg) proposed by Google [58], which parallelizes *Stochastic Gradient Descent* (SGD) on a small portion of clients, and the global model is the average of local model updates. To enhance it or to solve particular issues, several variants were proposed. The appropriate aggregation algorithm should be chosen based on the specific needs. For example, if privacy is very critical, *Secure Multi-Party Computation averaging* (SMC-Avg) [18] can be used. The *Federated Proximal* (FedProx) [54] and SCAFFOLD [44] are other examples of an aggregation algorithm that takes into account the client's heterogeneity. Finally, the server sends the global model to participant clients. *Communication* between server and clients can be in clear text or encrypted. Phases three and four are repeated until *convergence* is achieved, i.e., the model reaches a stable and optimal state, meaning it does not significantly change or enhance performance. Finally, after convergence, the global model can be used for detection.

There are three main *FL types* based on *data distribution* between clients: *Horizontal*, where datasets have similar features but different instances; *Vertical*, where datasets have the same instances but different features; and *Transfer* where the data of different clients differ both in the instances and the feature space, needed when collaboration is between different domains.

To assess the FL model, *evaluation* can occur either locally or at the server. The latter requires the utilization of public data to prevent the transmission of private data to the server. Evaluation metrics include *model metrics* like accuracy, precision, and recall and *system metrics* like resource consumption and communication overhead.

Many papers opt for a centralized architecture, implement supervised training on devices, and employ FedAvg for aggregation, chosen for their simplicity and compatibility with various applications. They generally do not use incentivizing or encryption mechanisms. Additionally, Horizontal FL is preferred for its similarity to distributed learning [50]. In the next section, we delve into FL-based IDSs in 5G, exploring whether they propose different parameters to address specific 5G challenges.

3 CURRENT STATE-OF-THE-ART OF FL BASED IDS APPROACHES IN 5G

Several approaches have leveraged FL to carry out intrusion detection for 5G. We examine them, and how they differ in their application domain, the challenges they solve, and the selected FL process. Figure 3 illustrates the taxonomy we propose for classifying FL-based IDS for 5G. This taxonomy encompasses 5G applications and characteristics, FL parameters outlined in the previous section, as well as the datasets utilized; specifically, it indicates whether the dataset was collected from a 5G network or for a specific use case, or if it is more general. We categorize papers based on their application use case to uncover challenges specific to each application and proposed solutions. This approach enables industries focusing on developing FL-based IDS for particular use cases to effectively adapt them. For every use case, we highlight the necessity of using

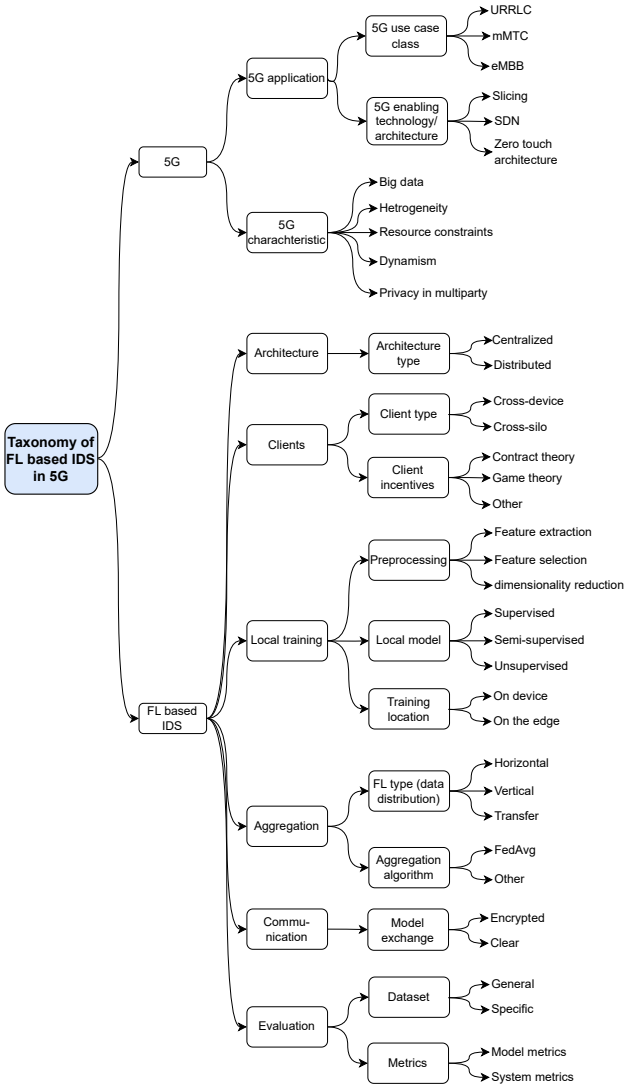

Figure 3: *Taxonomy for FL based IDS for 5G networks.*

5G technology. Subsequently, for each paper within this case, we outline any challenges addressed. We then discuss the adapted FL architecture and parameters, if they are different from the most used parameters. Finally, we delve into the model, dataset, and the results achieved by the researchers.

3.1 FL based IDS for URLLC use cases

In this use case, authors are interested in smart grids, vehicular networks, and *Cyber Physical Systems* (CPS).

3.1.1 Smart grids. They require reliable, high-speed, secure integration of diverse domains, making 5G technology essential because it provides reduced latency, improved connectivity, and slicing to cater to specific domain requirements. In the studies that we will discuss below [59, 70], the authors explore the development of a security system designed specifically for the advanced metering infrastructure (AMI) within 5G-enabled smart grids.

Sun et al. [70] describe a system using smart meters as intelligent sensors to communicate with household appliances via *Home Area Networks* (HANs). A *hierarchical FL* framework is proposed, where smart meters are grouped into clusters by 5G base stations. Each smart meter serves as an FL client. Updates are aggregated at the base station's edge server and then transmitted to the cloud server for further aggregation. This reduces communication costs compared to transmitting individual smart meter models directly. A *Transformer-IDM model* is introduced, comprising feature preprocessing and a detection model. Numerical features undergo convolutional and pooling operations for feature compression, while categorical features are embedded into a reduced-dimensional space and processed through transformer layers. They are concatenated and fed into a *Multi-Layer Perceptron* (MLP) for detection, achieving good performance, and outperforming competing models. The authors have left as *future work* addressing resource heterogeneity in FL and evaluating the model on datasets containing diverse attack types.

Mirzaee et al. [59]describe an FL architecture consisting of two layers: participants (households) training a Local IDS, and an FL server. The *detection method* uses one-hot encoding and a five-layered *Deep Neural Network* (DNN) classifier, achieving an accuracy of approximately 99.5% on the NSL-KDD dataset [71]. The authors suggest enhancing security with lightweight cryptography schemes and exploring the robustness of the federated IDS against fake reports.

3.1.2 Vehicular networks. Boualouache et al. [20] propose a scheme to detect passive mobile attackers in 5G vehicular edge computing. Passive attackers exploit wireless beacons, compromising privacy. These beacons, transmitted by vehicles, include crucial details such as the vehicle's identifier, position, and speed. Vehicular networks benefit significantly from 5G due to its low latency and high bandwidth. To *automate the labeling* process within the context of *vast data volumes* from 5G networks, the authors suggest a self-labeling mechanism. Here, labeled data are grouped into clusters, and unlabeled data are assigned labels according to these clusters. It is *evaluated* using synthetic data generated to emulate normal and attacker behaviors. Feature extraction relies on an inter-distance-based technique and various ML models are tested. Experimental results demonstrate the effectiveness, achieving a notable 95% accuracy with only twenty received beacons across 60 FL rounds.

In another effort by the same team [19], an FL approach is proposed to detect inter-slice attacks in 5G *vehicle-to-everything* (V2X) sliced networks by aggregating local models from each slice. To tackle the issue of *varying data distribution* among clients and prevent client non-participation due to this heterogeneity, the authors propose a game theory based incentive mechanism. In the problem formulation, the reward allocated to each vehicle is proportional to the data they contribute, also taking into account factors such as energy consumption and processing overhead. The *FL approach* includes three processes: inter-slice V2X attack detection process in the *New Radio* (NR) access technology, FL collaborative learning process at the MEC nodes, and FL global model update process at the 5G Core. For *evaluation*, they use the CSE-CIC-IDS-2018 dataset

[69] and a DNN model. They showcase high accuracy with varying numbers of clients.

Another study also addresses the detection of attacks in 5G *Cooperative Autonomous Vehicles* (CAVs) [48]. The *FL server* is situated in the MEC platform and the clients are CAVs. To tackle *labeling challenges* within big data, they adopt unsupervised learning using an autoencoder. *Evaluation* using realistic datasets [64] reveals promising detection performance with low false positive rates (FPR), even with a small number of participants.

The study by Rani et al. [66] examines the use of FL for detecting misbehavior in 5G-enabled *Internet of Vehicles* (IoVs). To *reduce communication overhead* and *address heterogeneity*, a *Federated Distillation* (FD) approach is used. Instead of transmitting the entire model, clients send only the average of predicted labels, minimizing data transmission in the network. Clients train the model individually, compute the average logits (outputs produced by the last layer of a neural network, before applying any activation function like softmax or sigmoid), set the average to zero if the label is unknown, and transmit these averages to the server that calculates a global average. In the *evaluation*, the FD-Scheme is compared with the FL-Scheme and previous works in the same field using a variety of datasets.

3.1.3 Cyber Physical Systems (CPS). A deep FL based IDS for industrial CPSs is proposed by Li et al. [51]. To ensure *security and privacy*, a secure communication protocol based on the Paillier cryptosystem is used to encrypt local model parameters. The *FL architecture* comprises a trust authority managing encryption, a cloud server (FL server), and industrial agents (FL clients). The *IDS* model incorporates a *Convolutional Neural Network* (CNN) and a *Gated Recurrent Unit* (GRU). Their system outperforms some state-of-the-art schemes.

3.2 FL based IDS for mMTC use cases

In this use case, authors are interested in Internet of Things (IoT) and Industrial IoT (IIoT) use cases.

3.2.1 IoT. In the realm of IoT, and to address *heterogeneity* between clients, IotDefender [30] use *Transfer Learning* (TL) to personalize clients' models by keeping the lower layers fixed and adjusting the parameters of the upper layers. To tackle the *restricted resources* issue in IoT devices, the training location is moved to the edge. Each IoT network sends its data to the corresponding MEC, which acts as the FL client. The 5G security cloud platform represents the FL server. IoTDefender is *evaluated* on five datasets and the federated TL outperforms standard TL in terms of generalization and identifying unknown threats with an 8.21% improvement. IoTDefender's tailored models for each IoT network have lower FPR. They highlight prospective *extensions* such as improving federation algorithms for poor network speeds and reacting to developing attack types via online incremental learning.

Similarly, the study by Man et al. [56] is designed for IoT networks. Their work improves upon FedAVG, drawing inspiration from attention mechanisms, by assigning different weights to clients depending on local data size. They also train their models on the edge to *reduce communication delay*. The proposed CNN model is *evaluated* on NSL-KDD and compared with centralized learning.

Finally, an IDS for 5G heterogeneous networks (HetNets) is proposed by Wei et al. [74]. Their *FL architecture* consists of attack detection nodes spread across three layers: end, edge, and cloud. In the end layer, powerful end nodes use deep reinforcement learning to identify attacks in their local access network. Due to restricted resources, they convey their results to edge nodes for aggregation. As an intermediate between the end and the cloud, the edge layer has complete knowledge of the access network and only limited awareness of the security of the core network. The cloud layer has a global view of the network's security and uses FL to aggregate model parameters from matching edge nodes. This method produces more accurate models for identifying various types of attacks. The proposed Deep Q-Network (D-QN) model, *evaluated* on the CICIDS2017 dataset [69], showcases superior performance in convergence speed and detection accuracy compared to non-cooperative, distributed ML, and traditional FL schemes.

3.2.2 IIoT. For IIoT heterogeneous Network, an IDS [4] is proposed with a focus on the Routing Protocol for Low-power and Lossy Networks (RPL). RPL serves as a routing protocol tailored for wireless networks characterized by low power consumption, typically vulnerable to packet loss. RPL uses a distance vector algorithm, specifically a variation of the objective function that computes paths based on certain metrics such as link quality, energy consumption, and expected transmission count. RPL is typically reactive or on-demand. It establishes routes in response to specific communication needs rather than continuously updating routes proactively. The Objective Function is a key concept in RPL. It defines the criteria for selecting and optimizing routes based on the specific requirements. To address the *heterogeneity* challenge, they adopt a Federated Transfer Learning-based Customized Intrusion Detection system called FTL-CID. The authors claimed that FTL-CID is the first model to apply FTL to a heterogeneous RPL-IIoT IDS security model. *Evaluated* on an RPL-IIoT dataset generated by simulation, FT-CID outperforms baseline models, particularly in small training sample sizes and federated environments, due to its ability to leverage knowledge from multiple datasets.

Verma et al. [73] also propose to secure IIoT networks by detecting *unknown attacks*. To do this, they train two models: one on normal traffic and the other on attack traffic. The framework utilizes a dual AE model to counter zero-day attacks, The model is trained and *evaluated* on the X-IIoTID dataset [6] representing real-world cybersecurity incidents. The results demonstrate that the proposed approach outperforms other methods, achieving high accuracy, detection rate, and F1 score.

3.3 FL based IDS for 5G enabling technologies

3.3.1 Zero touch architectures. To secure network and service management automation for 5G and beyond networks, an FL-based anomaly detection mechanism is proposed by Javasinghe et al. [40]. The automation requirements are addressed through the *Zero-touch Network and Service Management* (ZSM) framework, which integrates AI and ML algorithms. The INSPIRE-5Gplus project architecture [15] is used as a reference for ZSM. The suggested anomaly detection system is built in a hierarchical structure, to be easily incorporated into the ZSM architecture. The detecting procedure is divided into two steps. In the first stage, a basic ML model is

deployed within the security management domain to detect anomalies in network data. The second stage model benefits from a larger dataset and can tackle more complex problems, which improves overall detection accuracy. The study claims to be the first to propose a hierarchical FL-based anomaly detection mechanism for the ZSM architecture. *Evaluation*, done using the UNSW-NB15 dataset [60], demonstrates a minimum accuracy of 93.6%. Identified future work by authors aims to enhance accuracy further and integrate the model into a security analytics framework within the ZSM security architecture.

3.3.2 Softwarized networks. In the context of Softwarized Networks, an FL based IDS is presented by Aouedi et al. [11]. To overcome limitations due to labeling costs in 5G big data, the paper introduces a semi-supervised federated learning model for IDS. In this setup, clients in the network (edge nodes) train unsupervised models to learn representative features. The proposed autoencoder model is *evaluated* on the UNSW-NB15 dataset, achieving accuracy and detection rates of up to 84.32% and 83.10%, respectively, while maintaining data privacy with limited communication overhead.

3.3.3 Network slicing. Djaidja et al. [27] propose an FL based IDS where clients are 5G network slices. To address *data heterogeneity* caused by *non-independently and identically distributed* (non-IID) data between network slices, they investigate various aggregation algorithms such as FedAvg, FedProx, FedPer, and SCAFFOLD to evaluate their performance in both IID and non-IID scenarios. In 5G networks, data heterogeneity arises among different slices, as each slice is specific to a distinct domain. In non-IID settings, FedAvg and FedProx exhibit convergence difficulties, but SCAFFOLD outperforms FedProx and FedAvg. However, centralized models frequently outperform FL approaches, indicating that FL processes can be improved, particularly in non-IID settings. The NSL-KDD dataset is used for *evaluation* and is split randomly for IID settings and different percentages of attack types are attributed to different slices for non-IID. An MLP architecture with six layers is employed for model training, with hyperparameters set through testing.

Another paper, by Sedjelmaci et al. [68], also proposes a two-layer FL-based IDS to secure network slices in 5G. A *hierarchical* FL based IDS is presented. It consists of three systems structured into two layers. The first layer consists of defense systems at gNodeB nodes (base station) as FL clients and edge servers as FL servers. The second layer involves edge servers (FL clients) and the AMF as the FL server. To ensure robustness, a security model based on mean field games is proposed for the detection of *poisoning attacks*.

3.4 Discussion

Table 1 classifies the reviewed papers according to their 5G application domains, the challenges they address, as well as the corresponding FL variants employed along with evaluation dataset and metrics.

Among the surveyed articles, it appears that the mMTC class (IoT and IIoT) represents the most studied of the 5G classes. Researchers in the field of 5G are particularly interested in IoT due to its ubiquitous impact, market demand, and diverse applications. IoT represents a broad spectrum of interconnected devices and systems, spanning from smart homes and cities to industrial systems. Their scalability, and performance requirements make them compelling areas of research in 5G. 5G researchers are also keenly interested in vehicular networks and their security due to their transformative potential of connected vehicles. 5G security and reliability are paramount in vehicular networks and autonomous cars due to the critical nature of their operations and the potential risks associated. Smart grids are also studied since they benefit from 5G slicing, low latency, and speed. However, no application belonging to eMBB like virtual or augmented reality has been studied. The commercial deployment of VR and AR technologies has been progressing steadily even before the widespread availability of 5G networks. While 5G can certainly enhance the performance and capabilities of VR and AR applications, it may not be perceived as a critical enabler for their adoption compared to other use cases where 5G offers more transformative potential. For enabling technologies, there are two studies on slicing and one on softwarized networks while other technologies are completely ignored. Future research should explore the benefits of FL for these overlooked technologies.

The *FL framework* presented by McMahan et al. [58] is widely adopted in research. It typically employs a centralized, horizontal approach with cross-device capabilities, supervised learning for local training, and FedAvg for aggregation with some variants in weights as seen in Table 1. Nevertheless, the application of FL based IDS to 5G use cases faces several *challenges related to 5G* characteristics as explained earlier. The use of *appropriate FL variants* helps in addressing these challenges. For URLLC, especially in vehicular networks, challenges revolve around the substantial data volumes generated by 5G networks, leading to labeling concerns and heightened communication overhead. The former is tackled through self-labeling mechanisms or unsupervised learning, while the latter is mitigated via Federated Distillation, where only labels are exchanged. Additionally, heterogeneity in data distribution is managed by incentivizing parameters such as client participation. In mMTC scenarios, heterogeneity is managed through TL or by clustering similar clients. Moreover, due to the limited resources of IoT devices, many proposals move training towards the edge, thereby reducing communication delays. Enabling technologies like slicing and SDN face heterogeneity arising from slice differences through specific aggregation algorithms. Labeling issues are also tackled, and privacy concerns are reviewed, with techniques proposed to enhance privacy. However, there are other challenges to be considered. The dynamic nature of 5G networks makes it difficult to establish and maintain collaboration between different clients, as unstable clients may get replaced over time.

Vertical FL hasn't been adopted in the reviewed papers, despite its relevance in heterogeneous 5G environments. For example, implementing an IDS across different parties managing distinct network layers or architectural components in 5G (like CN and RAN) would ideally employ vertical FL. However, its limited use is due to challenges such as a lack of implementation tools and potential interoperability issues.

To evaluate proposed solutions, metrics related to detection, to FL process, and 5G characteristics are needed. While accuracy is a commonly used detection metric across various papers, some metrics like FPR are not consistently evaluated, despite their significance in assessing false positives that may lead to false alarms. System performance such as resource utilization and detection time,

Table 1: Classification of state-of-the-art papers proposing FL based IDS for 5G networks

Ref	5G							FL based IDS																														
	Applications			Challenges				Architecture			Client type		Client incentives		Prepro-cessing		Local model			Training location		Aggre-gation		Commu-nication		FL type			Dataset		Metrics	
	mMTC	URLLC	Enabling technology	Big data	Heterogeneity	Resources constraints	Privacy and security	Centralized	Centralized hierarchical	Decentralized	Cross-device	Cross-silo	Contract/not mentioned	Game theory	Feature extraction	Feature selection	Supervised	Semi-supervised	Unsupervised	On device	On the edge	FedAvg	Other	Clear	Encrypted	Horizontal	Vertical	Transfer	General	Specific	Model metrics	System metrics
[59]		x						x			x		x			x	x			x		x		x		x			x		x	x					
[70]		x							x		x		x		x		x			x		x		x		x			x		x	x					
[20]		x		x				x			x		x		x	x		x		x		x		x		x				x	x					
[48]		x		x				x			x		x		x				x	x		x		x		x			x		x						
[19]		x	x		x			x				x		x			x			x		x		x		x			x		x						
[30]	x				x	x		x			x		x				x				x	x		x				x	x	x	x						
[4]	x				x			x			x		x			x	x			x		x						x		x	x						
[74]	x				x			x			x		x				x				x	x		x				x	x								
[40]			x						x		x		x				x			x		x		x		x			x		x						
[11]			x	x				x			x		x					x		x		x		x		x			x		x						
[27]			x		x			x				x	x				x			x			x	x		x			x		x						
[66]		x		x				x			x		x		x		x			x		x		x		x			x	x	x						
[73]	x				x			x			x		x						x	x		x		x		x				x	x	x					
[65]	x							x			x		x				x			x		x		x		x			x		x						
[68]			x				x	x			x		x				x			x		x			x	x			x		x	x					
[56]	x			x				x			x		x				x				x	x		x		x			x		x						
[51]		x					x	x			x		x				x				x		x		x	x				x	x						

are less evaluated. As depicted in the table, the majority of papers employ general datasets, lacking specificity to 5G characteristics of the studied domain.

In the upcoming section, we will delve into each of IDS requirements in 5G, explore their implications in FL, and discuss potential solutions to bridge the existing gaps.

4 FL-BASED IDS CHALLENGES AND RESEARCH DIRECTIONS IN 5G

This section discusses 5G characteristics and the corresponding IDS challenges presented in Section 1 aiming to analyze gaps in the literature and propose solutions or alternative approaches. To achieve fast detection in 5G complex environments, it is imperative to streamline factors like optimizing communication costs, training durations, client selection methodologies, and hyperparameter selection [3, 24]. FL should also be scalable to handle 5G's massive and dynamic data and subscribers.

4.1 5G complexity and big data

The advent of 5G technology brings significant complexity and massive data generation, impacting IDS design. FL offers a distributed approach to model training without centralizing data, addressing data privacy concerns and reducing the load on central servers. However, it presents challenges for FL-based IDS in terms of process time, communication overhead, and scalability.

4.1.1 *Reducing FL process time.*

Reducing communication overhead. FL reduces communication overhead by eliminating the need to transmit data. However, the timeliness of FL-based IDS in highly complex environments with massive amounts of data remains a significant concern. Complex networks require substantial models, increasing the transmitted data volume. Additionally, the multitude of clients increases the number of exchanges with the central server, thereby augmenting communication overhead.

To guide research in this direction, some techniques proposed in other FL papers can be adopted for FL based IDS in 5G. For example, it is possible to reduce the total number of communication rounds and the number of transmitted messages at each round to mitigate this challenge and minimize communication overhead [54]. Several techniques such as model compression, gradient sparsification, local update aggregation, and adaptive communication frequency have been proposed [37, 79]. To evaluate the effectiveness of these techniques, they should be tested in a 5G application or simulation. 5G networks produce extensive data and integrate various characteristics that may not be typical in their use cases and evaluations.

Additionally, new techniques may be proposed in the future to further optimize the communication costs and enable real-time FL-based IDS in 5G networks.

Reducing training time. To expedite the training process in FL, several strategies can be employed. One approach involves restricting the number of local training epochs, thereby reducing the time taken in each FL round. Additionally, leveraging hardware accelerators such as GPUs or TPUs can significantly enhance the speed of model training, capitalizing on their parallel processing capabilities. Moreover, integrating machine learning optimization techniques like model pruning, which involves removing unnecessary parameters from the model, can further streamline the training process by reducing computational overhead and enhancing model efficiency.

Accelerating convergence. To expedite the convergence, several strategic approaches can be implemented. One such method involves the utilization of selective aggregation algorithms, which intelligently identify and prioritize the most pertinent updates from participating devices. Additionally, leveraging pretrained models during initialization can provide a valuable head start by initializing the model parameters close to their optimal values.

Preventing time loss in labeling. 5G applications generate vast amounts of data that require a non-negligible amount of time to be labeled. Unsupervised FL offers real-time analysis and rapid updates without the need for extensive labeling. Besides, unsupervised FL

enables continuous learning by allowing models to adapt to new data sources without requiring time-consuming manual annotation.

As mentioned earlier, Boualouache et al. [20] have proposed a semi-supervised FL-based 5G IDS using a self-labeling method. However, unsupervised FL IDS faces other 5G challenges, such as heterogeneity. This heterogeneity extends to the data generated by different network components, making clustering techniques, used in unsupervised learning, less effective. In FL, since we do not have access to training data and, in each iteration, clients train on their data separately, it is harder to determine a common baseline and clustering data to similar groups. Techniques to address heterogeneity will be presented in the next subsection.

4.1.2 Improving FL scalability to handle 5G's large and dynamic data. The rapid increase in both the number of devices and the amount of data generated in 5G networks presents a significant challenge for IDS. These systems need to be capable of processing a vast amount of traffic without sacrificing their ability to detect intrusions accurately and without being overloaded. *Decentralized FL* (DFL) eliminates the need for a central server. In DFL, the clients communicate directly with each other to train a global model. This can help improve the scalability of FL by reducing communication overhead, avoiding the need to exchange models of all clients with a central server, and eliminating the load on the server.

Other solutions can be considered. Proposing adaptive and dynamic client selection techniques is also essential for managing the varying and high number of 5G clients. For example, Chen et al. [25] treat scalability challenges in wireless networks based on resource constraints and possible packet losses. Due to bandwidth limits, the server in the base station must pick a subset of users for FL execution. The problem is stated as an optimization job.

4.2 5G heterogeneity

5G networks are diverse and this heterogeneity may have a profound impact on the performance of FL IDS across various dimensions, including data behavior heterogeneity, system heterogeneity, differences in confidentiality requirements and security policies, and insufficient involvement of clients due to data distribution heterogeneity between clients.

4.2.1 Addressing data and behavior heterogeneity using model personalizing techniques. Data and behavior heterogeneity is caused by domain heterogeneity and non-IID data. It can manifest in various ways, including non-identical distributions of characteristics or labels, common labels with different characteristics or common features with different labels, and unbalanced data sizes. Such heterogeneity can degrade model performance and increase the FPR [5]: within FL, all users employ a common global model that lacks specificity to their individual characteristics. This uniformity diminishes the effectiveness of attack detection and elevates the FPR.

To address this challenge, some techniques have been proposed, involving an initial collaborative training of the model followed by a personalized adaptation based on individual user characteristics [49]. For example, TL is used to personalize the FL model per client [4, 30]. Multi-task Learning [22] aims to solve more than one task at the same time. Meta-Learning [33] is a method that involves learning a model on a variety of tasks to handle new tasks with just few data [23]. Fallah et al. [29] use a model-agnostic meta-learning (MAML) in global training to obtain a personalized model. Finally, Knowledge Distillation [35] is a way to transfer knowledge from a large, complex model (teacher model) to a smaller and simpler model (student model). This allows the smaller model to enhance performance while remaining lighter and more suitable for deployment in resource-constrained areas.

However, some of these techniques have not been used in IDS FL, and only TL is used in a 5G scenario [30]. Besides, in 5G, there is an opportunity to experiment with these techniques to personalize the global model either by device or by network slice, as it facilitates grouping similar users or services.

4.2.2 Addressing differences in confidentiality requirements and security policies. In 5G, clients can be entities from different countries, companies, ISPs, or domains, each with their own security policies and confidentiality needs. This highlights the importance of considering the unique requirements of each entity when developing an IDS model. For instance, multiple organizations from different countries may work together to create an IDS model for 5G networks, and it is crucial to ensure that all requirements are met without compromising system performance or introducing conflicting rules [38]. These disparities may manifest in diverse ways, encompassing variations in confidentiality policies with differing levels of data sensitivity, discrepancies in access control policies, adherence to regulatory frameworks and data protection laws, distinctions in data sharing agreements, and divergent prioritization strategies.

Techniques to enhance privacy and reliability (against poisoning) in FL exist (Section 4.5), but careful selection is necessary to avoid conflicts between them. To address conflicting requirements among parties, clustering entities with similar needs can be effective. A hierarchical FL architecture, aggregating within clusters first and then across them, allows the selection of the most appropriate privacy and reliability mechanism without affecting other clusters.

4.2.3 Incentivizing FL IDS to Tackle Data Imbalances. The heterogeneous nature of 5G technology presents a critical challenge in encouraging client participation in FL. Typically, clients are motivated by the prospect of financial compensation or the opportunity to derive advantages from the converged global model. In cases where the resulting model is the primary benefit, which is the case in IDSs, it may not be fair. For instance, consider a group of ISPs collaborating to develop an IDS, where each ISP has a different number of subscribers with varying amounts of data. An ISP providing more data, logically, deserves more credit than other ISPs with less data. However, adhering to the FL paradigm as it is presented means that all ISPs will ultimately have the same model, which may be viewed as unfair and discourage participation. Furthermore, clients may be hesitant to participate in FL due to privacy concerns, resource limitations, network latency, and trust issues.

Addressing these concerns and creating fair incentive mechanisms is crucial for successful FL implementation in IDS. Techniques such as data augmentation enable parties with limited datasets to generate additional training instances. Furthermore, introducing incentive mechanisms, beyond mere financial compensation, such as access to advanced analytics, heightened security features, or

privileged model updates, can motivate participation and foster a more equitable FL ecosystem.

4.3 Resource constrained devices in 5G networks

FL helps in diminishing the necessity for centralized data storage and processing, thereby alleviating the demand for extensive computational and storage resources across all clients within a central entity. Nevertheless, the distributed nature of FL introduces a potential challenge: clients must possess sufficient local resources to conduct training for complex deep models. This reliance on local capabilities can become problematic when clients face constraints in terms of computational power and storage capacity. Limited resources can result in increased processing time.

4.3.1 FL with limited resources. While FL offers advantages in scalability and privacy, certain 5G devices, particularly IoT devices, may face limitations in processing power, bandwidth, and storage. FL encounters significant challenges in resource-constrained IoT environments [30]. First, communication overhead can be a major concern arising from large data sizes and non-optimized communication between servers and devices with limited bandwidth. Mobility, bandwidth constraints, and power limitations cause participant loss. FL *initially* assumes constant connectivity, which is impractical since participants may be disconnected and lost. A proposed solution involves evaluating the resource consumption of *stragglers* (nodes or devices that lag behind or take longer than planned to fulfill the tasks given to them) and adjusting local computation accordingly [26]. Another technique, deemed *asynchronous training*, updates the global model whenever a participant delivers a model update. Additionally, limited memory and energy budgets present obstacles to data storage. Besides, efficient training of DNNs needs powerful resources. The presence of IoT devices with inefficient processing units complicates the efficient communication and execution of ML algorithms. On-device training poses challenges related to model size and computing needs that may exceed the device's capability. Proposed solutions include tree-based algorithms for prediction on resource-constrained IoT devices, and dynamic computing technologies to regulate energy consumption during training. Challenges persist in extending battery life and developing aggregation algorithms suitable for low computational power and storage on IoT nodes like the use of TinyML [47]. The discourse also emphasizes hardware design advances, such as neuromorphic computing, to enhance efficiency [39].

4.3.2 Addressing resource constraints differences. FL in 5G faces system heterogeneity challenges due to the differences in storage, computing, and communication capabilities of devices (such as smartphones and IoT devices) involved in the training process. These differences can cause issues in synchronization and hyperparameters tuning such as determining the number of local and global epochs, training time, aggregation algorithm, and its parameters, especially in a 5G environment where real-time requirements need to be met and the environment is very dynamic. The conventional aggregation strategy used in FL may not be efficient on heterogeneous devices as it waits for slower devices to catch up before aggregating data.

Xu et al. [78] have identified several techniques used to improve model performance on heterogeneous devices and classified them into six categories. The first category is client selection, which involves selecting the most ready devices to participate in the training process. The second category is weighted aggregation, which involves assigning different weights to the updates received from each device by giving more weight to the updates from devices with higher computing power or better data quality. The third category is gradient compression, which involves compressing the updates sent by the devices to reduce communication costs. The fourth category is semi-asynchronous FL, which allows the devices to perform local updates at different times and speeds. The fifth category is cluster FL, which involves grouping the devices into clusters based on their similarities. The sixth category is model split, which involves splitting the ML model into smaller parts and distributing them among the devices. This technique helps to address the challenges associated with device heterogeneity by allowing each device to train the parts of the model that it is capable of handling depending on its available resources.

These techniques are yet to be tested in real-world scenarios by establishing scalable and flexible testbeds deployed on heterogeneous devices. Besides, dynamic resource allocation strategies should be explored to maximize training data size and engage the most interesting clients while respecting resource limits. *Proposing dynamic and adaptable techniques for asynchronous FL and how to generalize them for real-world scenarios is still an open direction.*

4.4 Dynamic 5G networks

FL allows for decentralized model training, making it suitable for dynamic environments where devices are highly mobile and may join or leave the network frequently. However, handling the dynamic joining and leaving of participants in FL poses challenges, especially in scenarios with high mobility.

Another challenge in these dynamic networks is concept drift [9] in FL which refers to the ML scenario where models are typically trained under the assumption that the distribution of data does not remain stationary. It means that the patterns and relationships learned from historical data are not expected to hold in future data. In 5G real-world applications, the data distribution may evolve due to various factors such as changes in user behavior, external events, or changes in virtual functions. The challenge of concept drift in FL is reinforced by the distributed nature of the FL paradigm. Clients may encounter concept drifts at varying times, and the characteristics of the drift may differ among clients. Conventional solutions assuming simultaneous or synchronized drifts are inadequate for this scenario. FL has no centralized authority or server possessing complete knowledge of the data across all clients. Consequently, centralized methods for handling drift may not be directly applicable. Adaptive aggregation algorithms are proposed to solve this challenge. For example, in 5G MEC, an attention mechanism is introduced by Estiri et al. [28] to dynamically adjust aggregation weights during model updates. The attention is on creating a global model that aligns with each local model in terms of weight distribution, to get the highest possible accuracy across all local data. Unlike conventional attention mechanisms, attention is applied to the learned parameters of neural networks in a layer-wise fashion.

In another approach, the process involves clustering to generate a distinct model for each novel concept. This enables clients associated with the same concept to train collaboratively [43]. The clustering may vary over time as concept drifts occur. Nonetheless, their clustering algorithm involves sharing local models with others, resulting in diminished privacy protection. Besides, the *coexistence of concept drift, anomalies, intrusions, and poisoning attacks* poses a challenge in adapting clustering algorithms appropriately. Additionally, future work should focus on collecting *real IDS datasets in 5G that can capture the variations of 5G traffic over time.*

4.5 Untrustworthy parties in 5G networks

Research in FL shows that it can be vulnerable to some integrity and confidentiality attacks which need to be addressed to meet 5G requirements. In this section, we explore these attacks, potential solutions, and open directions.

4.5.1 Reinforcing FL IDS privacy in 5G by mitigating inference attacks. The development of FL was driven by the need to enhance user privacy by keeping private data on the device where it was generated. However, *transmitted local model updates can reveal specific characteristics on the data.* These attacks, referred to as inference attacks, are classified into four types [34]: i) membership inference, which determines if a sample belongs to a specific class, ii) properties inference, which aims to obtain data properties, iii) training inputs and labels inference, and iv) class representative's inference, which uses *Generative Adversarial Networks* (GANs) to generate data similar to the original client's data by only accessing the model.

To address this issue in FL, several techniques have been proposed such as *Differential Privacy*, *Homomorphic Encryption* (HE), *Multi-Party Computation* (MPC) [81], and *Trusted Execution Environments* (TEEs) [5]. DP involves adding noise to client updates, which reduces an attacker's ability to extract information from sent updates. HE protects client data by performing calculations directly on ciphertexts, and MPC allows multiple parties with private data to compute a shared function without revealing their inputs. In 5G, a secure FL framework based on blockchain technology has been proposed by Liu et al. [55]. Their framework relies on smart contracts to prevent malicious or unreliable clients from participating in FL. Additionally, they use local DP techniques to prevent membership inference attacks. A hash graph-based FL method to defend against membership attacks through random sampling and noise addition is proposed by Kholidy et al. [46]. However, these approaches can impact the model's performance or require more processing power and a certain number of local participants to contribute to model training. The *privacy-enhancing technologies* (PET) can add computational and communication overhead and can also impact model performance. A study calculated the impact of different PET on the accuracy, training time, and network traffic [61] using two FL frameworks. For secure aggregation with Federated AI Technology Enabler (FATE), the values for accuracy, training time, and network traffic were approximately the same as those for FedAvg. However, with Paddle Federated Learning (PFL), there was a significant increase in network traffic and training time for certain settings. Specifically, for a batch size of 32, 10 rounds, and four clients, the network traffic with secure aggregation in PFL was 306 MB, compared to less than 30 MB with FedAvg. The training time was about 43 minutes with FedAvg and 56 minutes with PFL's secure aggregation. However, for other configurations, the differences were lower. For differential privacy in the PFL framework, the accuracy was reduced by about 10% for a batch size of 32. This poses challenges in some 5G applications characterized by limited resources or requiring rapid analysis. *To ensure practical effectiveness, researchers must strike a delicate balance between the need for privacy, accuracy, security, and overall system performance.* It is conceivable to implement personalization and clustering, e.g., by slice, wherein security mechanisms are chosen based on the specific requirements of each slice.

4.5.2 Mitigating poisoning attacks in an untrustworthy environment. Reliability is crucial in 5G applications, especially in the URLLC class. However, in FL, clients train local models, and data is not exchanged with the server, exposing a vulnerability for malicious clients to modify and poison data or local models without detection. Poisoning attacks can be targeted or untargeted, depending on the attacker's objective. Targeted attacks misclassify specific data without degrading model performance, making them more challenging to execute. An example of a targeted attack is injecting a backdoor against an FL-based IDS in a 5G IoT system, allowing the attacker to launch future network attacks without being detected. Other scenarios of poisoning attacks include distributed backdoor attacks (DBAs) [76], label poisoning attacks, model replacement [13], and adding noise or sign flipping [52].

In poisoning attacks, the attacker's gradients or models are either directly modified or trained on falsified data, resulting in updates that differ from those of other users. One mitigation approach consists then in eliminating updates that are far from others, which is the basis of robust aggregation algorithms such as Krum and multi-Krum [16], Trimmed Mean [80], Bulyan [36], Robust Aggregation for Federated Learning (RFA) [63], and Median [77]. These solutions calculate a score that measures the gradient distance, determining whether to discard or include updates depending on this score. Another approach involves evaluating the performance of a global model that incorporates the updates from a suspicious user against one that does not include these updates [31]. Additionally, some defenses clip the gradients' norm to reduce the impact of malicious workers, but at the cost of degrading the quality of honest updates [10]. Finally, methods that reverse the model updates using GANs have been proposed to reconstruct training participants' data and detect the attack [83]. This approach identifies the participant whose accuracy is lower than a predefined threshold as an attacker and removes their model parameters from the training procedure in that iteration. In 5G, to mitigate poisoning attacks, a blockchain is used where the central aggregator automatically executes smart contracts, which identify and isolate malicious and unreliable participants [55]. Other papers propose reputation-based strategies for reliable worker selection in the presence of low-quality or malicious devices [72].

While there have been many proposed solutions to mitigate poisoning attacks, it remains a difficult challenge in a *dynamic and heterogeneous 5G environment.* Solutions that are based on outliers can face challenges in determining what is a normal or a poisoned

update in a heterogeneous environment. Besides, this dynamic nature makes it challenging to establish trust among participants so solutions proposing giving a trust score will not be directly applicable. As a result, *finding robust methods to defend against poisoning attacks is an open research problem.* Additionally, some solutions pose privacy risks, such as those using GANs. *Future research efforts will need to focus on developing solutions that can simultaneously defend against poisoning attacks and preserve privacy* [75].

4.6 Lack of 5G datasets to evaluate FL based IDS

The lack of 5G datasets for evaluating FL-based IDS presents significant challenges in the field. Researchers often use non-5G datasets, which are general network traffic data collected in legacy IT networks as shown in Table 1, which lack 5G characteristics, and technologies. Although datasets collected from 5G networks or simulations do exist, they often lack the requisite attributes for effective IDS evaluation. Many such datasets predominantly feature legitimate network traffic without the inclusion of malicious or anomalous activities. It is worth considering whether existing 5G datasets can be repurposed and transformed into suitable datasets for IDS evaluation. This endeavor holds promise, albeit requiring intricate preprocessing and augmentation to include diverse instances of malicious activities representative of real-world threats. To facilitate the adoption of FL in IDS for 5G networks, there is a need to develop datasets conducive to distributed learning paradigms. These datasets should represent 5G network traffic and be able to partition and distribute across disparate client nodes in a realistic way.

5 CONCLUSION

This paper provides a comprehensive examination of the utilization of FL in IDSs for 5G networks. It emphasizes the importance of collaborative IDS in 5G networks due to new types of attacks, distributed attacks, and multi-party management. Yet, this collaboration introduces privacy concerns. FL addresses this by allowing local training on local devices, reducing communication overhead and resource usage on the central server. This study provides an overview of existing FL-based IDS classified by 5G application domain. It also delves into the specific 5G characteristics and examines the solutions proposed for the challenges arising from these characteristics. This includes the adjustment of FL processes and parameters, as well as the techniques employed in detection. However, certain challenges were either given inadequate attention or completely overlooked, underscoring the necessity for further research. Additionally, alternative solutions can be envisioned for those challenges that were addressed.

To boost FL IDS performance in complex 5G environments, challenges like communication overhead and scalability can be addressed using techniques such as model compression, gradient sparsification, and Decentralized FL. Unsupervised FL IDS is essential for real-time analysis, but it's more complex due to no data access and less efficiency in heterogeneous data. Heterogeneity introduces challenges related to data and behavior diversity, system differences, and confidentiality requirements. Techniques like clustering and personalization, such as TL, can be used. System heterogeneity, driven by resource constraints, can be tackled with solutions like data distribution, memory management, and innovative approaches for resource-constrained devices. Asynchronous FL allows training across devices with varying capabilities. Designing FL-based IDS for dynamic 5G networks faces challenges like participant changes and concept drift. Adaptive aggregation methods and clustering solutions can be used. Collaboration of untrustworthy parties in 5G raises privacy and security challenges, addressed by techniques like differential privacy. Similarly, a lack of trust causes poisoning attacks, that need effective mitigation.

ACKNOWLEDGMENTS

This work was carried out in the context of Beyond5G, a project funded by the French government as part of the economic recovery plan, namely "France Relance" and the investments for the future program. This work has been partially supported by the French National Research Agency under the France 2030 label HiSec (ANR-22-PEFT-0009). The views reflected herein do not necessarily reflect the opinion of the French government.

REFERENCES

[1] [n. d.]. FiGHT (5G Hierarchy of Threats). https://fight.mitre.org/. Accessed: 2023-07-24.

[2] [n. d.]. International Telecommunication Union Radio communication Sector (ITU-R). https://www.itu.int/en/ITU-R/Pages/default.aspx. Accessed: 2023-02-28.

[3] Sawsan AbdulRahman, Hanine Tout, Azzam Mourad, and Chamseddine Talhi. 2020. FedMCCS: Multicriteria client selection model for optimal IoT federated learning. *IEEE Internet of Things Journal* 8, 6 (2020), 4723–4735.

[4] Nasr Abosata, Saba Al-Rubaye, and Gokhan Inalhan. 2023. Customised Intrusion Detection for an Industrial IoT Heterogeneous Network Based on Machine Learning Algorithms Called FTL-CID. *Sensors* 23, 1 (2023), 321.

[5] Shaashwat Agrawal, Sagnik Sarkar, Ons Aouedi, Gokul Yenduri, Kandaraj Piamrat, Mamoun Alazab, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu. 2022. Federated learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications* (2022).

[6] Muna Al-Hawawreh, Elena Sitnikova, and Neda Aboutorab. 2021. X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial Internet of Things. *IEEE Internet of Things Journal* 9, 5 (2021), 3962–3977.

[7] Mohammed Jaber Alam, Md Rahat Hossain, Salahuddin Azad, and Ritesh Chugh. 2023. An overview of LTE/LTE-A heterogeneous networks for 5G and beyond. *Transactions on Emerging Telecommunications Technologies* 34, 8 (2023), e4806.

[8] Saqib Ali, Qianmu Li, and Abdullah Yousafzai. 2024. Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey. *Ad Hoc Networks* 152 (2024), 103320.

[9] Giuseppina Andresini, Feargus Pendlebury, Fabio Pierazzi, Corrado Loglisci, Annalisa Appice, and Lorenzo Cavallaro. 2021. Insomnia: Towards concept-drift robustness in network intrusion detection. In *Proceedings of the 14th ACM workshop on artificial intelligence and security*. 111–122.

[10] Galen Andrew, Om Thakkar, Brendan McMahan, and Swaroop Ramaswamy. 2021. Differentially private learning with adaptive clipping. *Advances in Neural Information Processing Systems* 34 (2021), 17455–17466.

[11] Ons Aouedi, Kandaraj Piamrat, Guillaume Muller, and Kamal Singh. 2022. Intrusion detection for softwarized networks with semi-supervised federated learning. In *ICC 2022-IEEE International Conference on Communications*. IEEE, 5244–5249.

[12] Sarhad Arisdakessian, Omar Abdel Wahab, Azzam Mourad, Hadi Otrok, and Mohsen Guizani. 2022. A survey on iot intrusion detection: Federated learning, game theory, social psychology and explainable ai as future directions. *IEEE Internet of Things Journal* (2022).

[13] Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. 2020. How to backdoor federated learning. In *International Conference on Artificial Intelligence and Statistics*. PMLR, 2938–2948.

[14] Aitor Belenguer, Javier Navaridas, and Jose A Pascual. 2022. A review of federated learning in intrusion detection systems for iot. *arXiv preprint arXiv:2204.12443* (2022).

[15] C Benzaid, P Alemany, D Ayed, G Chollon, M Christopoulou, G Gür, V Lefebvre, EM de Oca, R Munoz, J Ortiz, et al. 2020. White paper: Intelligent security architecture for 5g and beyond networks. *INSPIRE-5Gplus* (2020).

[16] Peva Blanchard, El Mahdi El Mhamdi, Rachid Guerraoui, and Julien Stainer. 2017. Machine learning with adversaries: Byzantine tolerant gradient descent. *Advances in Neural Information Processing Systems* 30 (2017).

[17] Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, Vladimir Ivanov, Chloe Kiddon, Jakub Konečnỳ, Stefano Mazzocchi, Brendan McMahan, et al. 2019. Towards federated learning at scale: System design. *Proceedings of Machine Learning and Systems* 1 (2019), 374–388.

[18] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. 2016. Practical secure aggregation for federated learning on user-held data. *arXiv preprint arXiv:1611.04482* (2016).

[19] Abdelwahab Boualouache and Thomas Engel. 2022. Federated Learning-based Inter-slice Attack Detection for 5G-V2X Sliced Networks. In *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*. IEEE, 1–6.

[20] Abdelwahab Boualouache and Thomas Engel. 2022. Federated learning-based scheme for detecting passive mobile attackers in 5G vehicular edge computing. *Annals of Telecommunications* (2022), 1–20.

[21] Enrique Mármol Campos, Pablo Fernández Saura, Aurora González-Vidal, José L Hernández-Ramos, Jorge Bernal Bernabé, Gianmarco Baldini, and Antonio Skarmeta. 2022. Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. *Computer Networks* 203 (2022), 108661.

[22] Rich Caruana. 1997. Multitask learning. *Machine learning* 28, 1 (1997), 41–75.

[23] Fei Chen, Mi Luo, Zhenhua Dong, Zhenguo Li, and Xiuqiang He. 2018. Federated meta-learning with fast convergence and efficient communication. *arXiv preprint arXiv:1802.07876* (2018).

[24] Hao Chen, Shaocheng Huang, Deyou Zhang, Ming Xiao, Mikael Skoglund, and H Vincent Poor. 2022. Federated learning over wireless IoT networks with optimized communication and resources. *IEEE Internet of Things Journal* 9, 17 (2022), 16592–16605.

[25] Mingzhe Chen, Zhaohui Yang, Walid Saad, Changchuan Yin, H Vincent Poor, and Shuguang Cui. 2020. A joint learning and communications framework for federated learning over wireless networks. *IEEE Transactions on Wireless Communications* 20, 1 (2020), 269–283.

[26] Anirban Das and Thomas Brunschwiler. 2019. Privacy is what we care about: Experimental investigation of federated learning on edge devices. In *Proceedings of the First International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things*. 39–42.

[27] Taki Eddine Toufik Djaidja, Bouziane Brik, Abdelwahab Boualouache, Sidi Mohammed Senouci, and Yacine Ghamri-Doudane. 2024. Federated Learning for 5G and Beyond, a Blessing and a Curse-An Experimental Study on Intrusion Detection Systems. *Computers & Security* (2024), 103707.

[28] Amir Hossein Estiri and Muthucumaru Maheswaran. 2021. Attentive Federated Learning for Concept Drift in Distributed 5G Edge Networks. *arXiv preprint arXiv:2111.07457* (2021).

[29] Alireza Fallah, Aryan Mokhtari, and Asuman Ozdaglar. 2020. Personalized federated learning: A meta-learning approach. *arXiv preprint arXiv:2002.07948* (2020).

[30] Yulin Fan, Yang Li, Mengqi Zhan, Huajun Cui, and Yan Zhang. 2020. Iotdefender: A federated transfer learning intrusion detection framework for 5g iot. In *2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE)*. IEEE, 88–95.

[31] Minghong Fang, Xiaoyu Cao, Jinyuan Jia, and Neil Gong. 2020. Local model poisoning attacks to {Byzantine-Robust} federated learning. In *29th USENIX Security Symposium (USENIX Security 20)*. 1605–1622.

[32] Elena Fedorchenko, Evgenia Novikova, and Anton Shulepov. 2022. Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges. *Algorithms* 15, 7 (2022), 247.

[33] Chelsea Finn, Pieter Abbeel, and Sergey Levine. 2017. Model-agnostic meta-learning for fast adaptation of deep networks. In *International conference on machine learning*. PMLR, 1126–1135.

[34] Romit Ganjoo, Mehak Ganjoo, and Madhura Patil. 2022. Mitigating Poisoning Attacks in Federated Learning. In *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2021*. Springer, 687–699.

[35] Jianping Gou, Baosheng Yu, Stephen J Maybank, and Dacheng Tao. 2021. Knowledge distillation: A survey. *International Journal of Computer Vision* 129, 6 (2021), 1789–1819.

[36] Rachid Guerraoui, Sébastien Rouault, et al. 2018. The hidden vulnerability of distributed learning in byzantium. In *International Conference on Machine Learning*. PMLR, 3521–3530.

[37] Pengchao Han, Shiqiang Wang, and Kin K Leung. 2020. Adaptive gradient sparsification for efficient federated learning: An online learning approach. In *2020 IEEE 40th international conference on distributed computing systems (ICDCS)*. IEEE, 300–310.

[38] Dirk Hetzer, Maciej Muehleisen, Apostolos Kousaridas, and Jesus Alonso-Zarate. 2019. 5g connected and automated driving: Use cases and technologies in cross-border environments. In *2019 European conference on networks and communications (EuCNC)*. IEEE, 78–82.

[39] Ahmed Imteaj, Urmish Thakker, Shiqiang Wang, Jian Li, and M Hadi Amini. 2021. A survey on federated learning for resource-constrained IoT devices. *IEEE Internet of Things Journal* 9, 1 (2021), 1–24.

[40] Suwani Jayasinghe, Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, and Mika Ylianttila. 2022. Federated learning based anomaly detection as an enabler for securing network and service management automation in beyond 5g networks. In *2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 345–350.

[41] Dajie Jiang and Guangyi Liu. 2016. An overview of 5G requirements. *5G Mobile Communications* (2016), 3–26.

[42] Ji Chu Jiang, Burak Kantarci, Sema Oktug, and Tolga Soyata. 2020. Federated learning in smart city sensing: Challenges and opportunities. *Sensors* 20, 21 (2020), 6230.

[43] Ellango Jothimurugesan, Kevin Hsieh, Jianyu Wang, Gauri Joshi, and Phillip B Gibbons. 2023. Federated learning under distributed concept drift. In *International Conference on Artificial Intelligence and Statistics*. PMLR, 5834–5853.

[44] Sai Praneeth Karimireddy, Satyen Kale, Mehryar Mohri, Sashank Reddi, Sebastian Stich, and Ananda Theertha Suresh. 2020. Scaffold: Stochastic controlled averaging for federated learning. In *International conference on machine learning*. PMLR, 5132–5143.

[45] Rabia Khan, Pardeep Kumar, Dushantha Nalin K Jayakody, and Madhusanka Liyanage. 2019. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials* 22, 1 (2019), 196–248.

[46] Hisham A Kholidy and Riaad Kamaludeen. 2022. An Innovative Hashgraph-based Federated Learning Approach for Multi Domain 5G Network Protection. In *2022 IEEE Future Networks World Forum (FNWF)*. IEEE, 139–146.

[47] Kavya Kopparapu, Eric Lin, John G Breslin, and Bharath Sudharsan. 2022. Tinyfedtl: Federated transfer learning on ubiquitous tiny iot devices. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. IEEE, 79–81.

[48] Abdelaziz Amara Korba, Abdelwahab Boualouache, Bouziane Brik, Rabah Rahal, Yacine Ghamri-Doudane, and Sidi Mohammed Senouci. 2023. Federated Learning for Zero-Day Attack Detection in 5G and Beyond V2X Networks. In *AlgoTel 2023-25èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications*.

[49] Viraj Kulkarni, Milind Kulkarni, and Aniruddha Pant. 2020. Survey of personalization techniques for federated learning. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. IEEE, 794–797.

[50] Léo Lavaur, Marc-Oliver Pahl, Yann Busnel, and Fabien Autrel. 2022. The evolution of federated learning-based intrusion detection and mitigation: a survey. *IEEE Transactions on Network and Service Management* 19, 3 (2022), 2309–2332.

[51] Beibei Li, Yuhao Wu, Jiarui Song, Rongxing Lu, Tao Li, and Liang Zhao. 2020. DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems. *IEEE Transactions on Industrial Informatics* 17, 8 (2020), 5615–5624.

[52] Liping Li, Wei Xu, Tianyi Chen, Georgios B Giannakis, and Qing Ling. 2019. RSA: Byzantine-robust stochastic aggregation methods for distributed learning from heterogeneous datasets. In *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 33. 1544–1551.

[53] Shancang Li, Li Da Xu, and Shanshan Zhao. 2018. 5G Internet of Things: A survey. *Journal of Industrial Information Integration* 10 (2018), 1–9.

[54] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. 2020. Federated optimization in heterogeneous networks. *Proceedings of Machine Learning and Systems* 2 (2020), 429–450.

[55] Yi Liu, Jialiang Peng, Jiawen Kang, Abdullah M Iliyasu, Dusit Niyato, and Ahmed A Abd El-Latif. 2020. A secure federated learning framework for 5G networks. *IEEE Wireless Communications* 27, 4 (2020), 24–31.

[56] Dapeng Man, Fanyi Zeng, Wu Yang, Miao Yu, Jiguang Lv, and Yijing Wang. 2021. Intelligent intrusion detection based on federated learning for edge-assisted internet of things. *Security and Communication Networks* 2021 (2021), 1–11.

[57] Lourenco Marco and Marinos Louis. 2019. ENISA threat landscape for 5G networks. In *Proc. Eur. Union Agency Cybersecurity (ENISA)*. 87.

[58] H Brendan McMahan, Eider Moore, Daniel Ramage, and Blaise Agüera y Arcas. 2016. Federated learning of deep networks using model averaging. *arXiv preprint arXiv:1602.05629* 2 (2016).

[59] Parya Haji Mirzaee, Mohammad Shojafar, Zahra Pooranian, Pedram Asefy, Haitham Cruickshank, and Rahim Tafazolli. 2021. FIDS: A Federated Intrusion Detection System for 5G Smart Metering Network. In *2021 17th International Conference on Mobility, Sensing and Networking (MSN)*. IEEE, 215–222.

[60] Nour Moustafa and Jill Slay. 2016. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. *Information Security Journal: A Global Perspective* 25, 1-3 (2016), 18–31.

[61] Evgenia Novikova, Dmitry Fomichov, Ivan Kholod, and Evgeny Filippov. 2022. Analysis of privacy-enhancing technologies in open-source federated learning frameworks for driver activity recognition. *Sensors* 22, 8 (2022), 2983.

[62] Ruxandra F Olimid and Gianfranco Nencioni. 2020. 5G network slicing: A security overview. *IEEE Access* 8 (2020), 99999–100009.

[63] Krishna Pillutla, Sham M Kakade, and Zaid Harchaoui. 2019. Robust aggregation for federated learning. *arXiv preprint arXiv:1912.13445* (2019).

[64] Rabah Rahal, Abdelaziz Amara Korba, and Nacira Ghoualmi-Zine. 2020. Towards the development of realistic dos dataset for intelligent transportation systems. *Wireless Personal Communications* 115, 2 (2020), 1415–1444.

[65] Sawsan Abdul Rahman, Hanine Tout, Chamseddine Talhi, and Azzam Mourad. 2020. Internet of things intrusion detection: Centralized, on-device, or federated learning? *IEEE Network* 34, 6 (2020), 310–317.

[66] Preeti Rani, Chandani Sharma, Janjhyam Venkata Naga Ramesh, Sonia Verma, Rohit Sharma, Ahmed Alkhayyat, and Sachin Kumar. 2023. Federated Learning-Based Misbehaviour Detection for the 5G-Enabled Internet of Vehicles. *IEEE Transactions on Consumer Electronics* (2023).

[67] Salman Rashid and Shukor Abd Razak. 2019. Big data challenges in 5G networks. In *2019 Eleventh international conference on ubiquitous and future networks (ICUFN)*. IEEE, 152–157.

[68] Hichem Sedjelmaci and Abdelwahab Boualouache. 2023. When Two-Layer Federated Learning and Mean-Field Game Meet 5G and Beyond Security: Cooperative Defense Systems for 5G and Beyond Network Slicing. *IEEE Transactions on Network and Service Management* (2023).

[69] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A Ghorbani. 2018. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSP* 1 (2018), 108–116.

[70] Xin Sun, Zhijun Tang, Mengxuan Du, Chaoping Deng, Wenbin Lin, Jinshan Chen, Qi Qi, and Haifeng Zheng. 2022. A Hierarchical Federated Learning-Based Intrusion Detection System for 5G Smart Grids. *Electronics* 11, 16 (2022), 2627.

[71] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. 2009. A Detailed Analysis of the KDD CUP 99 Data Set. http://www.unb.ca/cic/datasets/nsl.html.

[72] Aashma Uprety and Danda B Rawat. 2021. Mitigating poisoning attack in federated learning. In *2021 IEEE symposium series on computational intelligence (SSCI)*. IEEE, 01–07.

[73] Priyanka Verma, Nitesh Bharot, John G Breslin, Donna O'Shea, Ankit Vidyarthi, and Deepak Gupta. 2023. Zero-Day Guardian: A Dual Model Enabled Federated Learning Framework for Handling Zero-Day Attacks in 5G Enabled IIoT. *IEEE Transactions on Consumer Electronics* (2023).

[74] Yunkai Wei, Sipei Zhou, Supeng Leng, Sabita Maharjan, and Yan Zhang. 2021. Federated learning empowered end-edge-cloud cooperation for 5G HetNet security. *IEEE Network* 35, 2 (2021), 88–94.

[75] Geming Xia, Jian Chen, Chaodong Yu, and Jun Ma. 2023. Poisoning Attacks in Federated Learning: A Survey. *IEEE Access* 11 (2023), 10708–10722.

[76] Chulin Xie, Keli Huang, Pin-Yu Chen, and Bo Li. 2019. Dba: Distributed backdoor attacks against federated learning. In *International Conference on Learning Representations*.

[77] Cong Xie, Oluwasanmi Koyejo, and Indranil Gupta. 2018. Generalized byzantine-tolerant sgd. *arXiv preprint arXiv:1802.10116* (2018).

[78] Chenhao Xu, Youyang Qu, Yong Xiang, and Longxiang Gao. 2021. Asynchronous federated learning on heterogeneous devices: A survey. *arXiv preprint arXiv:2109.04269* (2021).

[79] Yang Xu, Yunming Liao, Hongli Xu, Zhenguo Ma, Lun Wang, and Jianchun Liu. 2022. Adaptive control of local updating and model compression for efficient federated learning. *IEEE Transactions on Mobile Computing* (2022).

[80] Dong Yin, Yudong Chen, Ramchandran Kannan, and Peter Bartlett. 2018. Byzantine-robust distributed learning: Towards optimal statistical rates. In *International Conference on Machine Learning*. PMLR, 5650–5659.

[81] Chen Zhang, Yu Xie, Hang Bai, Bin Yu, Weihong Li, and Yuan Gao. 2021. A survey on federated learning. *Knowledge-Based Systems* 216 (2021), 106775.

[82] Weishan Zhang, Qinghua Lu, Qiuyu Yu, Zhaotong Li, Yue Liu, Sin Kit Lo, Shiping Chen, Xiwei Xu, and Liming Zhu. 2020. Blockchain-based federated learning for device failure detection in industrial IoT. *IEEE Internet of Things Journal* 8, 7 (2020), 5926–5937.

[83] Ying Zhao, Junjun Chen, Jiale Zhang, Di Wu, Jian Teng, and Shui Yu. 2020. PDGAN: A novel poisoning defense method in federated learning using generative adversarial network. In *International conference on algorithms and architectures for parallel processing*. Springer, 595–609.