Elevating 5G Network Security: A Profound Examination of Federated Learning Aggregation Strategies for Attack Detection

Ioannis Makris
MetaMind Innovations
Kozani, Greece
imakris@metamind.gr

Nikolaos Ntampakis
MetaMind Innovations
Kozani, Greece
nntampakis@metamind.gr

Thomas Lagkas
International Hellenic University
Kavala, Greece
tlagkas@cs.ihu.gr

Panagiotis Radoglou-Grammatikis
University of Western Macedonia
Kozani, Greece
pradoglou@uowm.gr

Sotirios K. Goudos
Aristotle University of Thessaloniki
Thessaloniki, Greece
sgoudo@physics.auth.gr

Vasileios Argyriou
Kingston University London
London, UK
vasileios.argyriou@kingston.ac.uk

Eleftherios Fountoukidis
Sidroco Holdings LTD
Nicosia, Cyprus
efountoukidis@sidroco.com

Antonio F. Skarmeta
University of Murcia
Murcia, Spain
skarmeta@um.es

Pablo Fernandez Saura
University of Murcia
Murcia, Spain
pablofs@um.es

Panagiotis Sarigianndis
University of Western Macedonia
Kozani, Greece
psarigiannidis@uowm.gr

***Abstract*—The popularity of 5G networks has resulted in significant advancement and opportunities in connectivity and reliability of communications, but, concurrently, it raised security challenges and privacy concerns due to the distributed and highly dynamic nature of these networks. In particular, while participating devices and nodes in a 5G network need to be resilient against cyber threats, most of them are not allowed to exchange their data, and, therefore, they are limited only to the corresponding patterns identified locally. To tackle this, this paper proposes a federated learning approach to enable different nodes to collaboratively train a unified intrusion detection system while avoiding the direct exchange of data. In our experiments, we tested a number of different federated learning strategies with two (2) base stations that serve as participating clients in a federated learning scheme, while a server orchestrates the training phase. In terms of evaluation, the proposed solution was tested against the 5G-NIDD dataset and produced a high detection rate of 97.89% accuracy.**

***Index Terms*—5G, Federated Learning, Flower, Intrusion Detection Systems, Privacy, Security**

I. Introduction

The emerging evolution of communication technologies resulted in the introduction and integration of fifth-generation (5G) wireless networks in various aspects of life, offering significant advancements in connectivity, speed, reliability, and, overall, enhanced network capabilities. However, the rapid increase of interconnected devices, ranging from Internet of Things (IoT) environments to components of critical infrastructures, such as healthcare facilities [1], or large financial systems, that utilise 5G communications have raised certain concerns related to security and privacy [2], due to the fact that these 5G ecosystems are a potential surface of attacks for malicious actors [3]. In this context, the utilisation of an effective Intrusion Detection System (IDS) is of critical importance in any network's security structure. More precisely, an IDS serves as the main actor of every network's defense strategy, as it is capable of detecting both simple and advanced cyberattacks by closely monitoring the network traffic for abnormal activity or unauthorized access. Traditional IDSs, however, are significantly challenged by the dynamic and complex characteristics of 5G networks [4]. These challenges are directly connected with the advancements that 5G networks offer. Firstly, the heterogeneity of the diverse range of devices that participate in a 5G ecosystem in terms of communication protocols, or data formatting, demand a unified intrusion detection system that is able to keep track of all types of network communication traffic. Moreover, the vast majority of applications that incorporate 5G communications, such as autonomous vehicles, or industrial automation, require an extremely low latency. As a result, the IDS of these networks mandates that the traffic analysis and the detection of attacks must take place without producing any significant delays. The aforementioned challenge is highly correlated with the massive data volume of traffic that 5G networks can potentially generate. In particular, traditional IDSs may struggle to handle and monitor this large magnitude of data traffic, especially, in real-time, leading to significant delays in detecting threats. Finally, it is important to note that due to the diverse nature of the participating entities in a 5G network, such as individual users, large corporations, and/or public authorities, privacy concerns have been raised as the monitoring of the network traffic, and, as a result, the detection of potential attacks,

should take place within each user's privacy rights.

One emerging and promising solution to counter the aforementioned challenges is the development of an IDS in a Federated Learning (FL) approach. FL takes advantage of the decentralized nature of 5G networks across the different devices and network edges to collaboratively train an IDS without the need to share data between the participating nodes. This approach not only takes into account privacy concerns due to the fact that data remain at each node, where the training takes place but also increases the adaptability and detection capability of the whole system. Furthermore, the communication cost is significantly decreased, as data is not required to be transmitted through the network.

This paper aims to investigate the potential of FL-based learning IDSs in the context of 5G networks in order to best counter the aforementioned challenges, while, simultaneously, providing a high-performance threat detection rate. Additionally, in order to have a deeper analysis of FL utilisation in 5G networks, we conducted experiments using different FL aggregation strategies, providing insights into the level of influence that aggregation strategies have.

The rest of the paper is organised as follows: Section 2 provides a brief description of related works on FL-IDS in 5G networks. Section 3 describes the architecture of the proposed solution, while Section 4 presents the main characteristics of the dataset that was used for the evaluation. Section 5 illustrates the experimental setup and results of the proposed solution, and Section 6 concludes the paper with a summary of the most important aspects and provides directions for future research.

II. Related Work

In the context of securing 5G networks against rapidly evolving cyber threats, conventional and traditional approaches are encountering challenges such as privacy, scalability, and heterogeneity among others. As a result, the research community turned its attention towards more innovative solutions that can potentially address these challenges. More precisely, the concept of applying federated learning approaches in Intrusion Detection Systems showed extremely promising results, as without any reduction in the performance of the IDS, the participating nodes did not have to exchange any kind of data.

The IoT devices that are the main components of most 5G and edge computing architectures have limited resources, and, therefore, they are highly vulnerable to cyber-attacks. As Fan et al. describe in [5], three major challenges influence the security and privacy of 5G communications. The first challenge is located around the difficulty of training, but mostly designing a unified IDS due to the heterogeneity and diversity of IoT devices, and, in extend IoT networks. Next, the exchange of raw, or processed, data between nodes is not allowed in most cases due to privacy and security reasons. Finally, each participating device may not produce a high volume of data, making its corresponding IDS less reliable. To address these challenges, the authors designed an IDS for 5G IoT environments based on Federated Transfer Learning, called IoTDefender. In particular, the proposed solution is responsible for the aggregation during the FL procedures, implementing detection models utilising transfer learning, and, simultaneously, allowing the IoT devices to share information without leaking any sensitive data. Regarding the evaluation of the proposed framework, IoTDefender achieved an accuracy of 91.93%, higher than traditional methods, and, simultaneously, produced a lower false positive rate, demonstrating its generalisation ability.

With the main goal being the implementation and provision of resilient systems in the context of 5G Smart Grids, machine learning algorithms are utilised for the detection of intrusion by closely monitoring the incoming traffic flow. This approach requires the participating nodes to share their private data with a centralised entity, which is responsible for the training of the machine learning models. In order to keep each node's data private, Mirzaee et al. in [6] proposed a Federated Intrusion Detection System (FIDS) framework in 5G environments. More precisely, they developed a Federated Deep Neural Network (FDNN) that is trained using each node's data, and a server that performs the aggregation of the nodes' local training, and the distribution of the result of the aggregation back to the nodes. Regarding the evaluation of the proposed solution, it achieved a 99.5% accuracy, precision, recall, and F1-score using the NSL-KDD dataset.

It is undoubtful that there are significant advancements in mobile communications due to the development of 5G, and 6G technologies. However, along with this evolution, a number of more sophisticated and advanced attacks threaten the security, reliability, and privacy of these networks. Even though AI-enabled IDS have shown remarkable results in detecting attacks, the distributed nature of 5G, and 6G, environments requires the deployment of these systems to take place in a distributed manner, without any reduction in the performance. In doing so, Park et al. in [7] developed a split training approach that allows the training of such AI models to be in a distributed scheme. The proposed method was evaluated against the 5G-NIDD dataset and produced 96% accuracy.

In order to counter the high heterogeneity of networks, Popoola et al. in [8] proposed a Federated Deep Learning (FDL) architecture, in which the participating nodes train a deep Artificial Neural Network (ANN) using only local traffic flow. Additionally, they developed a server that is responsible for the aggregation of the resulting parameters of local training and the distribution of the updated model back to the nodes. Regarding the ANN architecture, it consists of the input layer, two hidden layers, and the output layer. Regarding the evaluation, the authors conducted a comparison between different federated aggregation strategies, and they found that FedAvg+ produced the best results with an accuracy of 99.27%, precision of 97.03%, recall of 98.06%, and F1-score of 97.50%.

While this was a brief presentation of related studies in the domain of IDS in FL environments, it is obvious that the need for an effective IDS which not only detects cyber-attacks, but preserves the privacy of sensitive data, and, simultaneously,

provides a resilient solution is vital. In the next section, the architecture of the proposed solution will be presented along with the dataset that it will be evaluated against and the corresponding results.

III. Architecture of the Proposed Solution

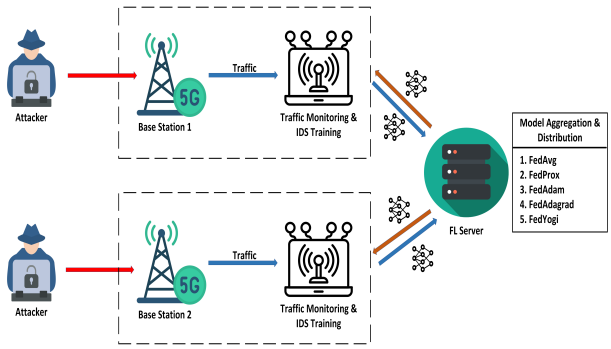

Fig. 1: Architecture of the proposed solution

In response to the challenge of providing an effective federated learning-based intrusion detection system that will be able to train an AI/ML model without exchanging data, this paper adopted the architecture shown in Fig. 1. More precisely, as illustrated in Fig. 1, a server that is responsible for the orchestration of the training phase coexists and communicates with the two (2) base stations and their corresponding devices that monitor the traffic and perform the IDS training that we treat as the federated learning clients. In this schema, each client (base station) trains an AI/ML model that it received from the server by only using data generated internally and then transmits back to the server the updated model. Then, the server is responsible for the aggregation of each client's model, using a pre-defined FL strategy. Finally, the server broadcasts back the aggregated model to the clients, completing one training round. The whole procedure is executed for a specific number of training rounds, or period of time.

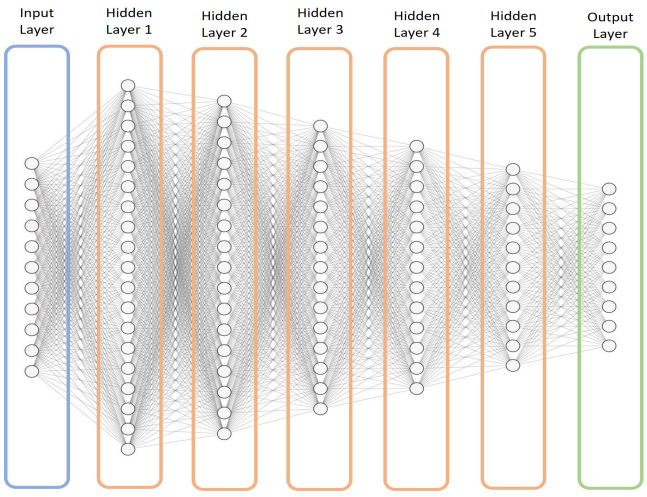

Fig. 2: Neural network architecture

Considering the AI/ML technique that was utilised, we designed and developed a custom Multi-Layer Perceptron (MLP). In particular, this MLP consists of five hidden layers, as shown in Fig. 2 with an output layer of nine (9) neurons, as the number of classes that are present in the dataset that we tested our solution. Each of the successive hidden layers has a gradually decreasing number of neurons starting at one hundred and fifty and ending at twenty-five. With nine different network attack type classes to forecast, we used a soft-max activation function to set up the output layer of the neural network.

Regarding the FL implementation, after the local training of the aforementioned MLP by each client, the resulting local model parameters are transmitted back to the server, where the aggregation will take place. With the main goal being the analysis of different federated learning strategies, we conducted experiments using the following strategies:

1) **FedAvg**. An FL strategy that performs a weighted average of local model updates [9].
2) **FedProx**. A generalisation of FedAvg, which introduces a proximal term, aiming to limit the impact of variable local updates [10].
3) **FedAdam**. An FL optimisation strategy which introduces two decay parameters, which control the importance that the algorithm will give to historical updates and the importance that will be given to current model updates [11].
4) **FedAdagrad**. An FL optimisation strategy that performs the aggregation based on the difference of each client model from the server's global model [11].
5) **FedYogi**. An FL optimisation strategy that aggregates the clients' models using the distance they have from the server's model, the direction of this difference (sign), and a decay parameter, as described above [11].

Our thorough exploration of these FL strategies in combination with the custom MLP that we designed, allowed us to comprehensively assess their suitability in the detection of attacks in 5G networks.

IV. Dataset Description

Under the needs of work performed for 5G-NIDD [12], the dataset was generated in an advanced environment centered around the 5G Test Network (5GTN) at the University of Oulu, Finland. This open ecosystem supports 5G technology research and was augmented with additional components for data collection. Notably, Nokia Flexi Zone Indoor Pico Base Stations formed the core, linked to attacker nodes, benign traffic devices, and a Dell N1524 switch. Raspberry Pi 4 Model B devices were configured as attackers, connected via Huawei 5G modems. An innovative approach involved capturing live traffic from real mobile devices, encompassing both attack and benign traffic. This dynamic environment laid the foundation for a dataset primed for realistic network intrusion detection analysis.

As a result, an extended data folder was created containing data both in packet-based and flow-based formats. The

data were collected from two base stations at each attack session separately and was stored in pcapng format. Also, a GPRS(General Packet Radio Service) Tunnelling Protocol (GTP) layer was removed from the data and the transformed data was saved PCAPNG (Packet Capture Next Generation), Argus, and CSV (Comma-Separated Values) file formats. The rest of the files include some concatenated versions of the initial files and also some encoded versions of them. Table I offers a summary overview of the produced files under the work performed for 5G-NIDD.

File Name	Format
Attackname_BSX.pcapng	pcapng
Attackname_BSX_nogtp.pcapng	pcapng
AttacknameX.argus	argus
AttacknameX.csv	csv
BTS_X.csv	csv
Combined.csv	csv
Encoded.csv	csv

TABLE I: All files in the 5G-NIDD dataset

To cater to the specific requirements of our study, we adapted our architecture to ensure that each client, symbolizing a base station, utilizes an appropriate dataset. As a result, we exclusively employed the datasets BTS_1.csv and BTS_2.csv to serve the objectives of our investigation. Both datasets include the same number of features, 52 in total, but a different number of rows, with BTS_1.csv containing 728,316 rows and BTS_2.csv containing 487,574 rows.

The features included in both datasets have to do with various aspects and metrics which observed during the attack sessions. Among these features, "Flgs" refers to the flags associated with network packets, "Seq" represents the sequence number of the packet and "Dur" and "RunTime" capture the times of the runtime of network flows. Various statistical attributes such as "Mean," "Sum," "Min," and "Max," are included in the dataset also. The protocol used is denoted by "Proto", while "sTos" and "dTos" stand for Type of Service (ToS) values. Attributes like "sDsb", "dDsb", "sTtl", "dTtl", "sHops" and "dHops" represent source and destination behavior flags, Time-to-Live values for source and destination and the number of hops taken by packets from source to destination accordingly. The feature "Cause" provides a cause code and the packet counts are represented by "TotPkts", "SrcPkts" and "DstPkts" while byte counts are captured by "TotBytes", "SrcBytes", and "DstBytes". Various load and loss metrics are also included in the dataset like "Load", "SrcLoad", "DstLoad", "Loss", "SrcLoss", "DstLoss", and "pLoss". "SrcGap" and "DstGap" signify time gaps. "Rate", "SrcRate" and "DstRate" denote transmission rates. Regarding state information the "State" feature is used, while TCP-related attributes include "SrcWin" and "DstWin" for TCP window sizes, "sVid" and "dVid" for VLAN IDs, and "SrcTCPBase" and "DstTCPBase" for TCP base values. Moreover, attributes like "TcpRtt", "SynAck" and "AckDat" provide insights into TCP Round-Trip Time and the presence of specific packet types. Finally, labels for attack identification ("Label"), attack types ("Attack Type"), and the tools used in attacks ("Attack Tool") complete the feature set.

In the context of our study, the "Attack Type" feature serves as our target variable. "Attack Type" encapsulates the diverse array of attack types present in the dataset (Table II), each characterized by distinct patterns and behaviors.

Attack Type	Description
Benign	Normal, non-malicious traffic
UDPFlood	Overload of UDP packets, leading to unresponsiveness due to "Destination Unreachable" replies
HTTPFlood	Mimics human behavior; Python Goldeneye tool deployed for application layer attack on Apache2 web server
SlowrateDoS	Exploits application layer with gradual attacks, evading detection. Slowloris establishes prolonged web connections, exhausting resources. Alternatively, the attacker sends false-size POST requests, stalling servers
TCPConnectScan	Mimics TCP handshake; full 3-way handshake performed
SYNScan	Scan uses SYN flag to detect open ports
UDPScan	Scans probes ports using UDP datagrams; open ports respond, non-UDP likely filtered
SYNFlood	Exploits TCP handshake; attacker sends SYN, exhausting receiver with half-open connections
ICMPFlood	Uses high-frequency ICMP echo requests, overwhelming services and network

TABLE II: Attack types in the 5G-NIDD dataset [8]

V. Experimental Evaluation

A. Experimental Setup

For the needs of our study, the experimentation configuration encompassed two local clients and a central server. Python was employed as the principal programming language, with the aid of numpy and pandas libraries for efficient dataset manipulation. TensorFlow facilitated the construction of the neural network architecture while the FL was realized through the integration with the Flower framework [13], enabling collaborative model training across different devices. It's important to note that the experiments ran on standard local PCs without high-end GPU capabilities.

B. Data Pre-processing

For the use of deep learning architectures, the utilization of datasets like BTS_1 and BTS_2 which exhibit characteristics like missing values and categorical features poses significant challenges in achieving an optimal model performance. In response, the formulation of a pre-processing pipeline emerged. This pipeline, tailored to the aforementioned needs, assumed a central role in our approach. What's more, its uniform implementation across the two distinct datasets not only ensured consistency but also provided a robust foundation for subsequent phases of model assessment. The proposed pre-processing pipeline encompassed several stages, each designed to enhance the quality and integrity of the data. By addressing the challenge of missing values, we carefully implemented strategies for handling them, whether through sample removal or imputation. We also took measures to ensure data fidelity

by eliminating duplicates, followed by the application of one-hot encoding techniques for effective feature representation. By recognizing the significant importance of feature scaling, we adopted the standard scaling approach to homogenize the disparate scales among attributes. Additionally, we addressed the concern of class imbalances in the "Attack Type" column by incorporating the the Synthetic Minority Over-sampling TEchnique (SMOTE) technique [14], ensuring comparability in distributions. Following the aforementioned steps, the BTS_1 dataset was refined to contain 3,655,341 samples, while the BTS_2 dataset was expanded to encompass 2,533,761 samples.

C. Evaluation Results

Regarding the performance evaluation, and given the nature of our problem as a 9-class classification, we used some of the most common evaluation metrics like confusion matrix, accuracy, and F1 score. The confusion matrix for our "Attack Type" classification problem is a structured representation that quantifies the performance of our MLP model in the context of federated learning by presenting the average - per class - clients' count of true positive (TP); count of instances where the model correctly predicts a sample belonging to a specific attack type as that exact one, true negative (TN); count of instances where the model correctly predicts a sample as not belonging to a specific attack type and it indeed does not belong to that type, false positive (FP); count of instances where the model predicts a sample as a specific attack type, but in reality, the sample does not belong to that attack type and false negative (FN); count of instances where the model fails to predict a sample as a specific attack type, even though the sample actually belongs to that attack type.

It's noteworthy to mention that due to variations in the number of evaluation data samples of each client, the evaluation metrics were computed using appropriate weights to ensure fair assessment, by accounting for each client's different contributions to the overall evaluation. Based on the outcomes derived from the confusion matrix, we calculated accuracy and F1 score, in (1) and (2) respectively, as essential indicators of our model's efficacy in handling the multi-class classification task.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$F1 = \frac{2 \times TP}{2 \times TP + FP + FN} \tag{2}$$

As mentioned above, for the needs of the federated learning analysis, we tested a range of different techniques. FedAvg and FedProx focus on the aggregation of model updates from local clients to improve model convergence and generalization when FedAdam, FedAdagrad and FedYogi integrate optimization techniques, aiming to enhance the model aggregation process by considering factors such as adaptive learning rates, and historical and current model updates. The exploration of federated learning techniques encompassed a sequence of 10 iterative training rounds, where an evaluation protocol was established to evaluate the models produced at the end of each round using the aforementioned metrics.

Strategy	Evaluation Metric	Client 1	Client 2	Average
FedAvg	Accuracy	99.45%	95.64%	**97.89%**
	F1-Score	99.45%	95.55%	**97.85%**
FedProx	Accuracy	82.22%	97.18%	88.35%
	F1-Score	79.01%	96.33%	86.11%
FedAdam	Accuracy	76.05%	75.12%	75.67%
	F1-Score	73.47%	72.97%	73.27%
FedAdagrad	Accuracy	78.35%	77.87%	78.15%
	F1-Score	73.22%	74.76%	73.85%
FedYogi	Accuracy	79.18%	75.49%	77.67%
	F1-Score	74.00%	71.01%	72.77%

TABLE III: Experimental results - Best model per strategy

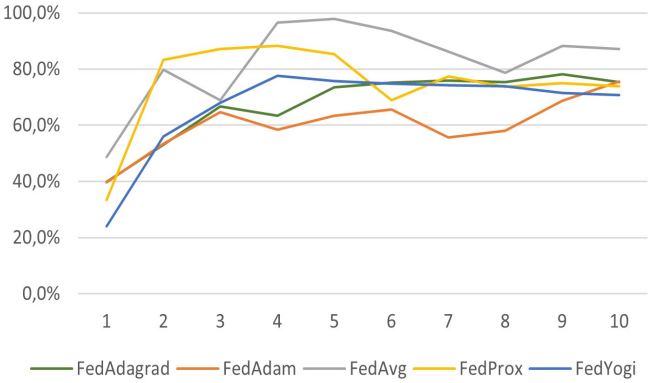

Fig. 3: Clients' average accuracy per round

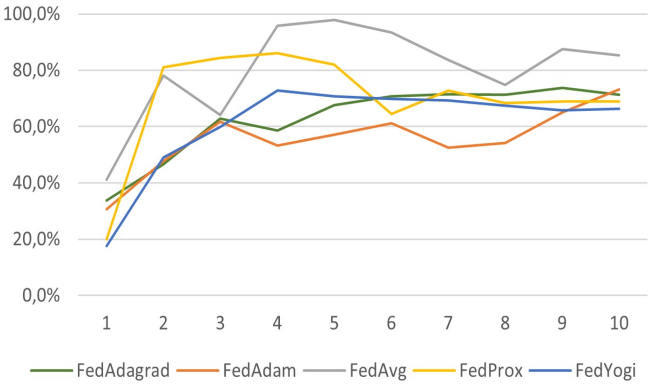

Fig. 4: Clients' average F1 score per round

Table III shows the best model that emerged for every federated learning strategy per client, and the average of them. Additionally, Fig. 3 and Fig. 4 show the clients' average accuracy and F1-score through the training phase.

As illustrated in Table III, FedAvg had the highest performance, compared to the other strategies. In particular, FedAvg achieved an average 97.89% accuracy and 97.85% F1-score. It is important to note that the second best strategy was

FedProx producing an average 88.35% accuracy and 86.11% F1-score. On the other hand, federated optimisation strategies did not perform well overall. Finally, in order to have a more complete analysis, we present the confusion matrix of the FedAvg experiment that achieved the best results in Fig. 5. The visual representation in Fig. 5 illustrates the system's ability in efficiently distinguishing between benign network traffic and a variety of attack types. Notably, the only salient observation arises from a limited number of instances where UDPFlood attacks are incorrectly classified as benign network flow.

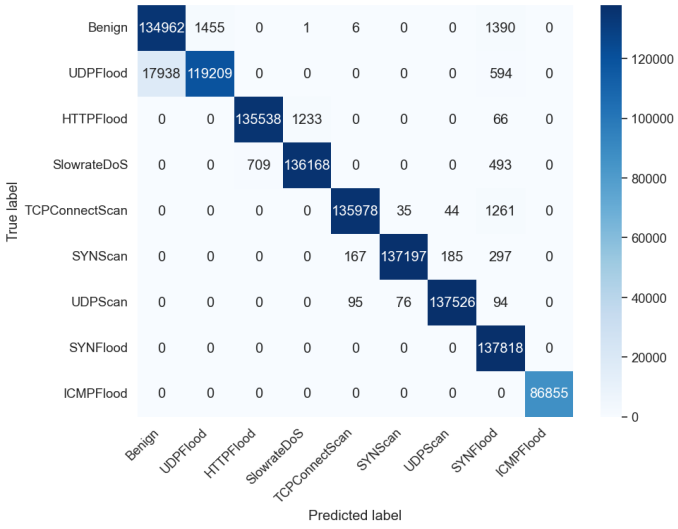

Fig. 5: FedAvg Confusion matrix

VI. Conclusions & Future Work

In the realm of 5G networks, where concerns regarding the privacy of sensitive data, and the security of the systems have significantly raised, the need for solutions that can address these important challenges is vital. This paper adopted a Federated Learning approach where multiple base stations collaboratively trained a deep ANN, without exchanging their corresponding data, but only the network's parameters at each training round. Additionally, we performed an investigation on different federated aggregation strategies from simple averaging to optimisation algorithms as they can highly influence the training phase of federated learning, and, to an extent, the performance of the model. As shown in the experimental results, FedAvg achieved the highest accuracy and F1-score with the federated optimisation strategies having the poorest performance. As a result, we conclude that intrusion detection systems that follow a federated learning approach can be treated as a highly resultful solution for detecting attacks in 5G networks.

Moving forward, the attention should be on defining new and more innovative federated aggregation strategies that are tailored to detecting intrusions aiming to optimise both the communication and the computation efficiency of a federated learning system. Furthermore, the exploration of practical and large-scale scenarios and the execution of corresponding experiments will both prove the feasibility of the proposed solution and, simultaneously, reveal any drawbacks of it.

Acknowledgment

This work has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096456 (NANCY). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or SNS JU. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, T. Lagkas, G. Fragulis, and A. Sarigiannidis, "A self-learning approach for detecting intrusions in healthcare systems," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[2] A. N. Mwang'onda and M. Phiri, "Comprehensive survey study on fifth-generation wireless network and the internet of things," *EAI Endorsed Transactions on Internet of Things*, vol. 9, no. 3, 2023.

[3] G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, S. Ouzounidis, M. Zevgara, I. Moscholios, S. Goudos, and P. Sarigiannidis, "Towards securing next-generation networks: Attacking 5g core/ran testbed," in *2022 Panhellenic Conference on Electronics & Telecommunications (PACET)*. IEEE, 2022, pp. 1–4.

[4] V. Perifanis, N. Pavlidis, R.-A. Koutsiamanis, and P. S. Efraimidis, "Federated learning for 5g base station traffic forecasting," *Computer Networks*, p. 109950, 2023.

[5] Y. Fan, Y. Li, M. Zhan, H. Cui, and Y. Zhang, "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, 2020, pp. 88–95.

[6] P. H. Mirzaee, M. Shojafar, Z. Pooranian, P. Asefy, H. Cruickshank, and R. Tafazolli, "Fids: A federated intrusion detection system for 5g smart metering network," in *2021 17th International Conference on Mobility, Sensing and Networking (MSN)*. IEEE, 2021, pp. 215–222.

[7] C. Park, K. Park, J. Song, and J. Kim, "Distributed learning-based intrusion detection in 5g and beyond networks," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2023, pp. 490–495.

[8] S. I. Popoola, G. Gui, B. Adebisi, M. Hammoudeh, and H. Gacanin, "Federated deep learning for collaborative intrusion detection in heterogeneous networks," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, 2021, pp. 1–6.

[9] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*. PMLR, 2017, pp. 1273–1282.

[10] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," *Proceedings of Machine learning and systems*, vol. 2, pp. 429–450, 2020.

[11] S. Reddi, Z. Charles, M. Zaheer, Z. Garrett, K. Rush, J. Konečnỳ, S. Kumar, and H. B. McMahan, "Adaptive federated optimization," *arXiv preprint arXiv:2003.00295*, 2020.

[12] S. Samarakoon, Y. Siriwardhana, P. Porambage, M. Liyanage, S.-Y. Chang, J. Kim, J. Kim, and M. Ylianttila, "5g-nidd: A comprehensive network intrusion detection dataset generated over 5g wireless network," *arXiv preprint arXiv:2212.01298*, 2022.

[13] D. J. Beutel, T. Topal, A. Mathur, X. Qiu, J. Fernandez-Marques, Y. Gao, L. Sani, K. H. Li, T. Parcollet, P. P. B. de Gusmão *et al.*, "Flower: A friendly federated learning research framework," *arXiv preprint arXiv:2007.14390*, 2020.

[14] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "Smote: synthetic minority over-sampling technique," *Journal of artificial intelligence research*, vol. 16, pp. 321–357, 2002.