DDoS attack detection using unsupervised federated learning for 5G networks and beyond

Saeid Sheikhi
and Panos Kostakos
University of Oulu
Faculty of Information Technology and Electrical Engineering
Center for Ubiquitous Computing
Finland 90570
Email: Saeid.Sheikhi@oulu.fi

***Abstract*—The rapid expansion of 5G networks, coupled with the emergence of 6G technology, has highlighted the critical need for robust security measures to protect communication infrastructures. A primary security concern in 5G core networks is Distributed Denial of Service (DDoS) attacks, which target the GTP protocol. Conventional methods for detecting these attacks exhibit weaknesses and may struggle to effectively identify novel and undiscovered attacks. In this paper, we proposed a federated learning-based approach to detect DDoS attacks on the GTP protocol within a 5G core network. The suggested model leverages the collective intelligence of multiple devices to efficiently and privately identify DDoS attacks. Additionally, we have developed a 5G testbed architecture that simulates a sophisticated public network, making it ideal for evaluating AI-based security applications and testing the implementation and deployment of the proposed model. The results of our experiments demonstrate that the proposed unsupervised federated learning model effectively detects DDoS attacks on the 5G network while preserving the privacy of individual network data. This underscores the potential of federated learning in enhancing the security of 5G networks and beyond.**

I. Introduction

Anticipated advancements in the fifth (5G) and sixth (6G) generations of mobile and communication networks are expected to yield significant improvements in speed, reliability, and network capacity [1]. These communication networks rely on connecting an immense number of devices and users, which leaves them to a wide range of privacy and security concerns that threaten the stability and trustworthiness of such networks [2].

Significantly, retrofitting machine learning (ML) in cybersecurity solutions has been highlighted as a critical research challenge in the upcoming age of beyond 5G and 6G networks. To overcome this research obstacle, real-time deep learning must be applied at the packet and byte levels. This leap forward will catalyze the advancement of the next generation of network-based intrusion detection (NIDS), host-based intrusion detection (HIDS), and Security Orchestration, Automation and Response (SOAR), resulting in the ability to autonomously detect and respond to security incidents [3]. Furthermore, with reference to the newly proposed Service of Services 6G Architecture [4], it is envisaged that these cyber security tools will be seamlessly integrated into the fabric of *Ubiquitous Intelligence*, creating a service that has the ability to self-configure, self-heal, self-protect, and self-optimize.

Notably, Distributed Denial of Service (DDoS) attacks are critical security issues targeting 5G networks. DDoS attacks are acknowledged as one of the critical risks facing network services due to their intimate, uncomplicated, and effective qualities. The GPRS Tunneling Protocol (GTP) protocol, which is extensively used in 5G networks, is a prime target for DDoS since it performs essential tasks, including session management and data transmission [5]. The severity of DDoS attacks and the damage they could inflict by flooding 5G networks, combined with their high level of automation and coordination (i.e., using DDoS botnets), has increased the need for reliable and efficient methods of detecting, preventing and mitigating such attacks.

Machine learning-based intrusion detection systems (ML-IDS) could play a substantial role in protecting large-scale systems by accurately detecting intrusions and generalizing this knowledge to recognize previously unseen threats (i.e., zero-day attacks) [6]. However, traditional centralized ML-based intrusion detection systems, which are frequently deployed in data silos, encounter certain limitations in detecting the latest security threats in fluid networks. These limitations stem from inadequate data integration, limited accessibility, and suboptimal data quality for training and testing purposes. To address this issue, in this research, we have tested a new IDS design that uses Federated Learning (FL) to detect DDoS attacks across 5G core networks. The FL models use the collaborative learning technique, which enhances the performance of traditional centralized ML models. This allows numerous devices, that might be deployed in data or network silos, to collaboratively learn a model without sharing the data, which helps to protect security and privacy devices on a large scale. Below is a summary of the main contributions.

- Introducing an unsupervised federated model approach for detecting DDoS attacks targeting the GTP protocol in 5G core networks.

- Designing an internet/public-facing 5G network testbed architecture.
- Simulating DDoS attacks in a realistic 5G core environment and collecting data from the extracted features within the network.
- Enhancing the evaluation of the model's performance by deploying it on the testbed and conducting experiments using real-world datasets and scenarios.

In terms of organization, this paper is structured as follows: Section II includes a review of the literature and findings from previous studies employing various techniques. Section III describes the process and development of the testbed, as well as the collection of datasets used in the experiment. Section IV introduces the unsupervised federated learning model for detecting DDoS attacks. Section V demonstrates the experimental setup and provides an analysis of the results obtained using the developed method. Finally, Section VI presents our summaries, conclusions, and suggestions for future work.

II. Related work

In recent years, security issues and vulnerabilities in 5G networks have attracted significant attention. Previous research has explored methods to improve the efficacy of anomaly detection in 5G networks using a variety of approaches, including centralized and federated learning. Therefore, this section provides an overview of the progress made in 5G network security as reported in recent literature.

Maimo et al. [7] proposed a 5G-focused architecture that utilizes deep learning (DL) to identify cyber-attacks. The study leverages the 5G network infrastructure, known as ETSI-NFV. The authors used the botnet dataset CTU to study 5G anomaly detection and employed the Long Short-Term Memory (LSTM) model as the DL technique. The outcomes were satisfactory for classifying and evaluating traffic in 5G environments. Monge et al. [8] introduced a novel 5G anomaly detection system called FlowSentinel. This method was implemented on SELENET on an ETSI-NFV 5G network ecosystem. In this study, the Machine learning model examines the outgoing flows in a 5G environment to detect the characteristics of malicious activity and devices conducting flooding-based DDoS attacks. Initial reports on the results show that DDoS activities were efficiently distinguished from regular activities.

Polat et al. [9] presented an ML-based model to detect DDoS attacks on 5G software-defined networks (SDN). The study utilized a dataset that encompassed the specific attributes from DDoS attacks and regular traffic in an SDN. The authors compared the efficiency of four ML techniques: Support Vector Machines (SVM), NB (Naive Bayes), ANN (Artificial Neural Network), and KNN (K-Nearest Neighbors) with feature selection. The testing findings demonstrated that KNN with wrapper feature selection approach achieved the best performance, with 98.3% accuracy. Li et al. [10] proposed a novel intelligent Intrusion Detection System with enhanced software-defined 5G architecture. The authors utilized KDD Cup 1999 and NSL-KDD datasets to test the system's performance. With balanced dataset training, the combination of the K-means++ and Adaboost algorithms performed better than other considered methods.

Accordingly, prior research indicates that machine learning methods can be employed to address security concerns in 5G networks. However, the traditional ML methods suffer from certain shortcomings, which can cause issues in detecting different types of attacks on a large scale. As a solution, it is suggested to adopt distributed learning methods such as the FL framework, which can perform better than centralized models in detecting DDoS attacks in 5G networks. Consequently, in this study, we proposed an unsupervised FL model to detect DDoS attacks in 5G core networks. The proposed model holds great promise for deployment and usage in protecting large-scale 5G network infrastructure against various threats.

TABLE I
The list of notations in the paper

Notation	Definition
AUSF	Authentication Server Function
AMF	Access and Mobility Management Function
UPF	User Plane Function
UDM	Unified Data Management
UDR	Unified Data Repository
PCF	Policy and Charging Function
SMF	Session Management Function
RAN	Radio Access Network
UE	User Equipment

III. Methodology

A. Notations

Various notations will be used to represent different concepts and variables throughout the paper. Table I reports a summary of these notations along with their respective definitions.

B. The 5G testbed

To establish a modern distributed cyber range and evaluate the real-world deployment of the federated learning model within a highly realistic 5G network environment, we designed and built 5G networks using Open5GS and UERANSIM. The 5G networks implemented in this study virtualize the 5G core network, providing the necessary infrastructure for

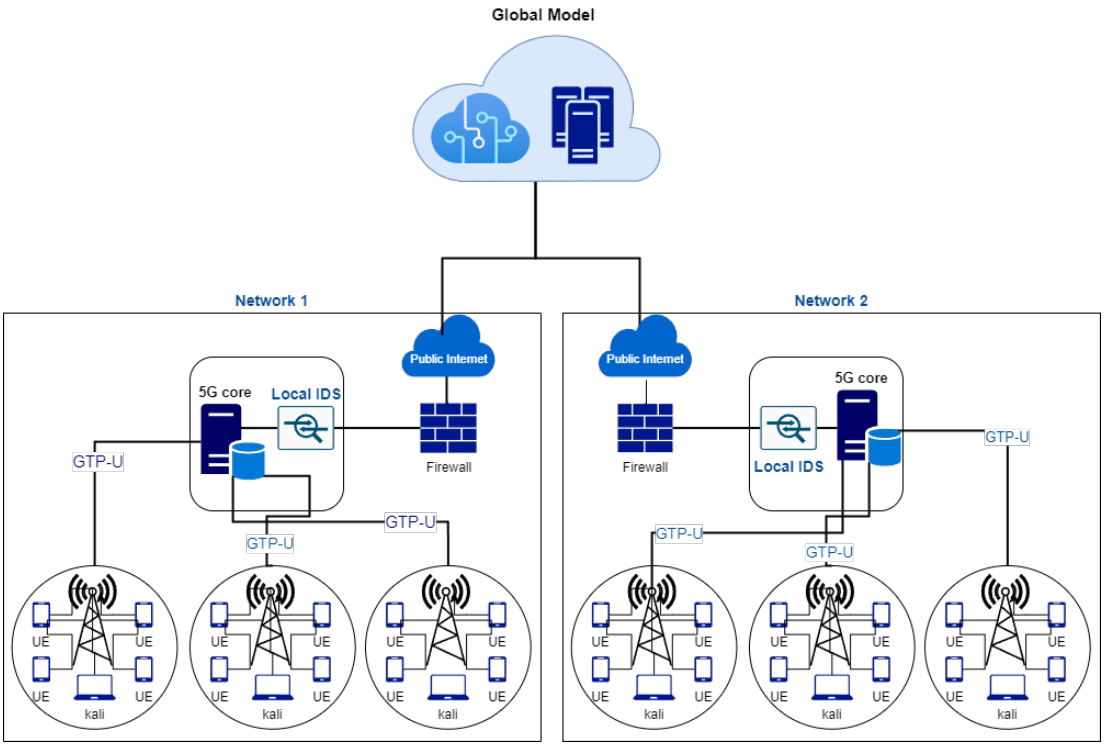

Fig. 1. The proposed model development and deployment architecture.

deploying the proposed model, simulating attack scenarios, and collecting the GTP packets. The architecture of the 5G networks used in the study is shown in Figure 1.

C. GPRS Tunneling Protocol

GPRS Tunneling Protocol (GTP) is a communication protocol for transmitting network data in mobile networks using IP [11]. In a mobile network, a GTP tunnel is constructed and established to deliver the data between the mobile client and the Internet. The packets generated by the client are encapsulated in the GTP-U (GTP User Plane) header by the gNB and transmitted to UPF through a GTP tunnel [12]. The G-protocol data unit (G-PDU) is composed of the encapsulated packet and the GTP-U header [13]. When packets are received, the system determines the optimal route to the Internet by comparing the destination IP address with the entries in the routing table. The architecture of the 5G system utilized in this study is depicted in Figure 2.

D. Attack scenarios simulation

DDoS attacks can significantly affect the security and reliability of 5G services [14]. For each 5G core network, we used three nodes to simulate realistic DDoS attacks. As shown in Figure 1, to build the federated model, each 5G has three base stations, and User Equipment (UE) are connected to the 5G core through these base stations. Three malicious nodes, each connected to a different gNB, are constructed for each 5G core in order to automate DDoS attacks on the network. Malicious node groups automatically launch the two most destructive Dos attacks, SYN flood and UDP flood, against the 5G core network.

SYN flood: A SYN flood, which is frequently produced by botnets, is made to overuse the target server's resources, such as the firewall or other perimeter security components [15]. It sends SYN packets at high rates to exceed service capacity limitations and bring them down. The first group of malicious nodes in the scenario launches this attack on the first 5G core network.

UDP Flood: A UDP flood attack occurs when an attacker exploits a large variety of source IPs to simultaneously transmit small, fake UDP packets to multiple ports on the targeted system [16]. As a result, the system's vital resources are getting used up and overloaded with high rates of incoming UDP packets. UDP attacks frequently do not follow a constant pattern, making them challenging to detect and stop. In the implemented scenario, the second group of malicious nodes launches this attack on the second 5G core network.

E. Feature extraction

The feature extraction process starts by collecting the GTP packets on the 5G core under the developed 5G network testbed described in the previous subsection. The collected GTP packet features are extracted using Tshark. The extracted features from packets are labeled and converted to the CSV format. The packets have various features, and not all features have a high correlation in detecting malicious activity in the network. Therefore, based on prior similar experiments [6], we conducted a comprehensive analysis to determine the most

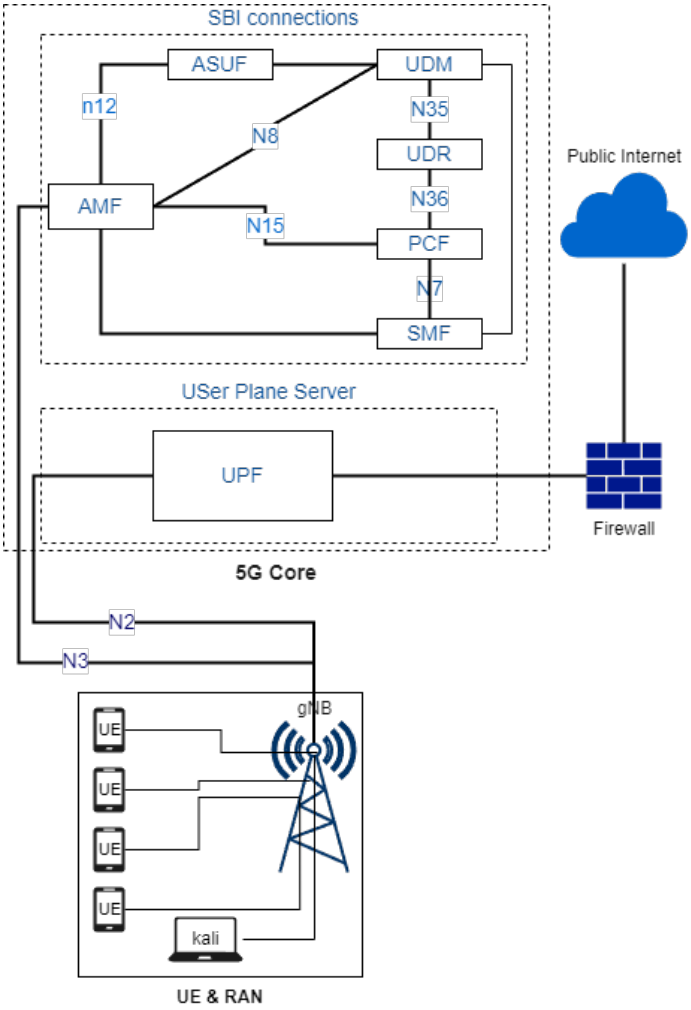

Fig. 2. The developed 5G network architecture.

efficient set of features that would improve the performance and reduce the processing time. The extracted features belong to different protocols, including GTP-U, TCP, and UDP. The list of extracted features is reported in Table II.

F. Data collection and Pre-processing

The extracted features were stored in CSV files and prepared for use in the proposed model. In this study, we used two 5G cores in the designed 5G testbed environment. Therefore, we split the collected data for each core. The DDoS data collected for SYN flood are used in the model deployed on the first 5G core, while the UDP flood dataset are prepared to be used on the second 5G core. However, the performance of the federated model was evaluated using test data that uses both types of DDoS attacks on 5G cores. The summarized information of the collected data is reported in Table III.

IV. Proposed Model

Federated Learning (FL) is a burgeoning learning scheme based on collaboratively decentralized technology, desiring to tackle data sensibility and data silos problems [17]. It

TABLE II
List of Extracted Features from the Network

Feature name	Feature name
ip.len	frame.time_relative
ip.flags.df	frame.time_delta
ip.flags.mf	tcp.time_relative
tcp.port	tcp.time_delta
tcp.window_size	gtp.ext_hdr
tcp.ack_raw	gtp.ext_hdr.length
ip.fragment.count	gtp.ext_hdr. pdu_type
ip.ttl	gtp.ext_hdr.pdu
ip.proto	qos_flow_id
tcp.ack	pdu_ses_cont.ppp
tcp.seq	gtp.ext_hdr.pdu
tcp.len	gtp.flags
tcp.stream	gtp.flags.e
tcp.urgent_pointer	gtp.flags.payload
tcp.flags	gtp.flags.pn
tcp.analysis.ack_rtt	gtp.flags.reserved
tcp.segments	gtp.flags.s
tcp.reassembled.length	gtp.flags.version
http.request	gtp.length
udp.port	gtp.message
udp.length	gtp.teid

TABLE III
Class Distribution in the Network Traffic Dataset

Class	Records
Benign	14932
SYN flood	10000
UDP flood	10000
Total records	34932

coordinated numerous clients (such as edge devices, organizations, and institutions) using one or multiple central servers in decentralized ML settings [18]. The global model aggregates clients' model parameters and transmits the updated model between the FL server and the distributed FL clients to attain an optimal level of accuracy. Tensorflow Keras library creates the proposed FL framework and develops and trains ML models on the client 5G cores. We utilized the Federated Averaging technique (FedAvg) for the server-side aggregation process.

In the proposed method, we take advantage of Autoencoder, which is an unsupervised machine learning (ML) model for detecting DDoS attacks. Autoencoder is frequently utilized to

extract features and reduce the dimension in high-dimensional data. The encoding and decoding are used to train the autoencoder network. While the decoder recovers compacted low-dimensional content to rebuild the output, the encoder often compresses the input into a latent-space representation. An unsupervised autoencoder is good choice for DDOS detection since it does not require labeled data for training and can successfully capture the underlying patterns and structures of network communication data. This is crucial for DDOS detection because labeled data might not always be accessible or might be expensive to collect. The model integrates an unsupervised autoencoder as a part of the federated learning architecture, allowing the model to be trained distributed across various clients while maintaining the confidentiality of the data. The autoencoder is distributed to each client and the server, and a federated technique is used to train the model. Each client uses its individual data to train the autoencoder, and it regularly communicates with the global server to update the overall model weights and parameters. After collecting the client updates, the server broadcasts the updated global model to the clients for more training. The model training process repeated until it converges to the best level of accuracy. The structure of the proposed FL model is shown in Figure 3.

The suggested model contains a number of processes, which are shown in Figure 1. In the first, the client models deployed on each 5G core are trained locally on their train dataset. Then, the weights and parameters are sent to the global model, which is deployed in the cloud for aggregation. Finally, the global model aggregates clients' weights and parameters on the server and updates the local models.

V. Experiment and Results Analysis

This section outlines the experimental setup and analyzes the test results using the proposed approach. It covers the process of the experiment, including its setup, performance metrics, and a thorough analysis of the results.

A. Experiment setup

This study employs the use of Python Keras and TensorFlow to implement the proposed model and pre-processing phases. The proposed federated model was implemented using the Flower framework and consisted of three training rounds. In the model the optimal level of accuracy by fine-tuning the global model's with each model local training dataset. Metrics like the loss function or accuracy is utilized to evaluate the efficacy of the model. The detection accuracy counts the percentage of successfully identified abnormal traffic, whereas the loss function reflects the percentage of differences between the actual output with predicted output. The loss function is a useful measure of the model's overall efficacy. An improved prediction of the output values for the training data is indicated by a reduced loss value, which typically translates to an enhanced accuracy on unseen data. The pre-processing and preparation of the dataset was carried out on a device equipped with an Intel Core i9 processor and 64G DDR4 memory. Specifically, in dataset pre-processing, we cleaned the dataset and filled the *nan* and *null* values. In addition, the global server is deployed on a cloud Linux machine with 8 Vcore and 16G running memory.

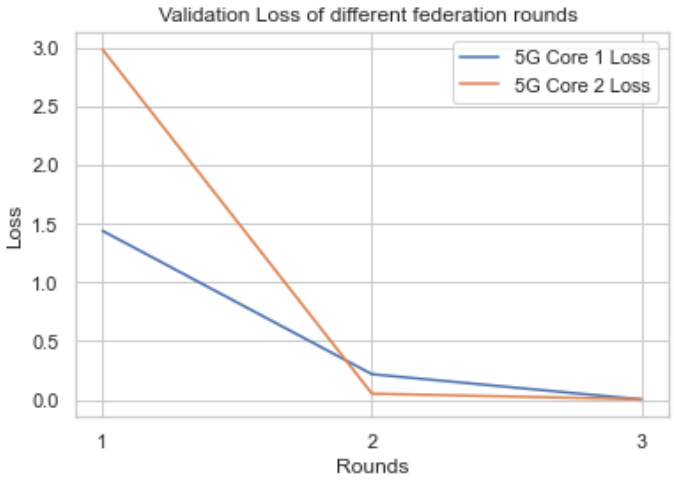

Fig. 3. The loss of models in each round of federated evaluation.

TABLE IV
Performance Evaluation of 5G core clients

Client	Accuracy	F1-score
5G Core 1	0.9986	0.9988
5G Core 2	0.9988	0.9990

B. Result analysis

In the attack scenarios, we configured to have two 5G cores, each receiving a specific type of DDoS attack. The proposed model is deployed in each 5G core to detect the attacks on the network. Figure 3 shows the loss values of the model in each 5G core for every round of the evaluation of the federation of the model. As the figure shows, the models start with a high loss rate since each model only has one type of DDoS attack. The initial loss rate for the model in 5G core 1 was around 15%, and for the 5G core 2, it is around 30%. However, after the models send their weights and parameters to the global server for aggregation and receive the updated model, the loss rate in both models improves significantly, decreasing to 2% and 5% for models in 5G core 1 and 5G core 2, respectively.

To report the FL model's performance in detecting DDoS attacks in both 5G cores, we used standard metrics, such as Accuracy and F1-score. Table IV reports the overall performance of the models in each 5G core after three rounds of weights and parameters aggregation. According to the represented results, both models performed well in distinguishing the DDoS attacks from regular packets, and both achieved over 99% accuracy.

A confusion matrix table is also used to show how well models are performed. The confusion matrix presents the actual and predicted values and demonstrates how many records

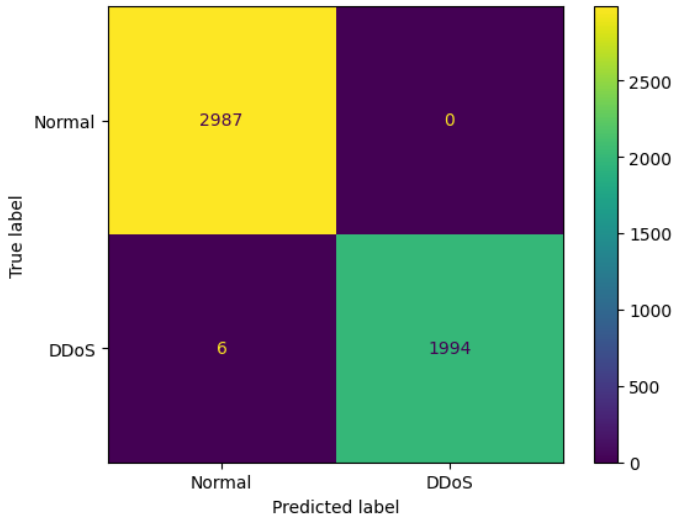

Fig. 4. The confusion matrix.

are correctly and incorrectly categorized. The confusion matrix of the model is illustrated in Figure 4.

VI. Conclusion and Future work

In this paper, we proposed an unsupervised federated learning-based approach to detect DDoS attacks on the 5G core network. The proposed method is based on an Autoencoder model and has been shown to effectively identify attacks on the 5G network. To run the experiments, we designed an internet/public-facing 5G testbed architecture featuring multiple 5G cores systems. The test environment that was built in this study was utilized to produce both malicious and normal traffic, based on the threat scenarios that were conducted. The suggested model was also evaluated on the testbed. Experiments results demonstrated that the suggested method performed well and could distinguish the DDoS packets with a high detection rate. It also demonstrates the capabilities of federated learning for security systems in 5G networks since it enables security systems collaboratively learn while preserving privacy.

This study aims to encourage future research and reinforce continuing efforts to tackle the increasing security concerns in 5G networks. In future work, it is recommended to develop and evaluate federated learning models against various types of cybersecurity threats in 5G networks, as well as investigate the integration of the proposed model with other security measures to improve the security in 5G networks. In order to establish a comprehensive understanding of the efficiency of the federated learning approach, we suggest further evaluation of the model against traditional machine learning models.

Acknowledgment

This research has been funded by the European Commission grant IDUNN (101021911) and the Academy of Finland 6G Flagship (318927).

References

[1] C. R. Storck and F. Duarte-Figueiredo, "A survey of 5g technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles," *IEEE access*, vol. 8, pp. 117 593–117 614, 2020.

[2] A. Al-Ansi, A. M. Al-Ansi, A. Muthanna, I. A. Elgendy, and A. Koucheryavy, "Survey on intelligence edge computing in 6g: characteristics, challenges, potential use cases, and market drivers," *Future Internet*, vol. 13, no. 5, p. 118, 2021.

[3] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. H. Nguyen, F. Liu, T. Hewa, M. Liyanage *et al.*, "6g white paper: Research challenges for trust, security and privacy," *arXiv preprint arXiv:2004.11665*, 2020.

[4] T. Taleb, C. Benzaïd, M. B. Lopez, K. Mikhaylov, S. Tarkoma, P. Kostakos, N. H. Mahmood, P. Pirinen, M. Matinmikko-Blue, M. Latva-Aho *et al.*, "6g system architecture: A service of services vision," *ITU journal on future and evolving technologies*, vol. 3, no. 3, pp. 710–743, 2022.

[5] Y. Kim, Y. Kim, and H. Kim, "A comparison experiment of binary classification for detecting the gtp encapsulated iot ddos traffics in 5g network," *Journal of Internet Technology*, vol. 23, no. 5, pp. 1049–1060, 2022.

[6] S. Sheikhi and P. Kostakos, "A novel anomaly-based intrusion detection model using psogwo-optimized bp neural network and ga-based feature selection," *Sensors*, vol. 22, no. 23, p. 9318, 2022.

[7] L. F. Maimó, Á. L. P. Gómez, F. J. G. Clemente, M. G. Pérez, and G. M. Pérez, "A self-adaptive deep learning-based system for anomaly detection in 5g networks," *Ieee Access*, vol. 6, pp. 7700–7712, 2018.

[8] M. A. S. Monge, A. H. González, B. L. Fernández, D. M. Vidal, G. R. García, and J. M. Vidal, "Traffic-flow analysis for source-side ddos recognition on 5g environments," *Journal of Network and Computer Applications*, vol. 136, pp. 114–131, 2019.

[9] H. Polat, O. Polat, and A. Cetin, "Detecting ddos attacks in software-defined networks through feature selection methods and machine learning models," *Sustainability*, vol. 12, no. 3, p. 1035, 2020.

[10] J. Li, Z. Zhao, and R. Li, "Machine learning-based ids for software-defined 5g network," *Iet Networks*, vol. 7, no. 2, pp. 53–60, 2018.

[11] J.-M. Tilli and R. Kantola, "Data plane protocols and fragmentation for 5g," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2017, pp. 207–213.

[12] Z. Cong, Z. Baokang, W. Baosheng, and Y. Yulei, "Ceupf: Offloading 5g user plane function to programmable hardware base on co-existence architecture," in *Proceedings of the 2021 ACM International Conference on Intelligent Computing and its Emerging Applications*, 2021, pp. 34–39.

[13] T. A. Navarro do Amaral, R. V. Rosa, D. F. C. Moura, and C. Esteve Rothenberg, "Run-time adaptive in-kernel bpf/xdp solution for 5g upf," *Electronics*, vol. 11, no. 7, p. 1022, 2022.

[14] A. S. Mamolar, P. Salvá-García, E. Chirivella-Perez, Z. Pervez, J. M. A. Calero, and Q. Wang, "Autonomic protection of multi-tenant 5g mobile networks against udp flooding ddos attacks," *Journal of Network and Computer Applications*, vol. 145, p. 102416, 2019.

[15] P. Kumar, M. Tripathi, A. Nehra, M. Conti, and C. Lal, "Safety: Early detection and mitigation of tcp syn flood utilizing entropy in sdn," *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1545–1559, 2018.

[16] U. Gurusamy and M. MSK, "Detection and mitigation of udp flooding attack in a multicontroller software defined network using secure flow management model," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 20, p. e5326, 2019.

[17] L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," *Computers & Industrial Engineering*, vol. 149, p. 106854, 2020.

[18] S. P. Ramu, P. Boopalan, Q.-V. Pham, P. K. R. Maddikunta, T.-H. The, M. Alazab, T. T. Nguyen, and T. R. Gadekallu, "Federated learning enabled digital twins for smart cities: Concepts, recent advances, and future directions," *Sustainable Cities and Society*, p. 103663, 2022.