Citation: G. Amponis, P. Radoglou-Grammatikis, G. Nakas, S. Goudos, V. Argyriou, T. Lagkas, and P. Sarigiannidis, "5G core PFCP Intrusion Detection Dataset", 2023 12th International Conference on Modern Circuits and Systems Technologies (MOCAST), Athens, Greece, 2023, pp. 1-4, doi: 10.1109/MOCAST57943.2023.10176693.

5G Core PFCP Intrusion Detection Dataset

George Amponis[†‡], Panagiotis Radoglou-Grammatikis[†§], George Nakas[†],
Sotirios Goudos[¶], Vasileios Argyriou[‖], Thomas Lagkas[‡] and Panagiotis Sarigiannidis[§]

***Abstract*—The rapid evolution of the 5G environments introduces several benefits, such as faster data transfer speeds, lower latency and energy efficiency. However, this situation brings also critical cybersecurity issues, such as the complex and increased attack surface, privacy concerns and the security of the 5G core network functions. Therefore, it is evident that the role of intrusion detection mechanisms empowered with Artificial Intelligence (AI) models is crucial. Therefore, in this paper, we introduce a labelled security dataset called *5GC PFCP Intrusion Detection Dataset*. This dataset includes a set of network flow statistics that can be used by AI detection models to recognise cyberattacks against the Packet Forwarding Control Protocol (PFCP). PFCP is used for the N4 interface between the Session Management Function (SMF) and the User Plane Function (UPF) in the 5G core. In particular, four PFCP attacks are investigated in this paper, including the relevant network traffic data in terms of pcap files and the Transmission Control Protocol (TCP)/Internet Protocol (IP) and application-layer statistics. This dataset is already publicly available in IEEE Dataport and Zenodo.**

***Index Terms*—5G, Artificial Intelligence, Cybersecurity, Intrusion Detection, PFCP**

I. Introduction

In today's communication landscape, there is a growing demand for secure and reliable connections with high-speed, high-throughput capabilities between the User Equipment (UE) and the Data Network (DN). The 5G core architecture, which follows the 3rd Generation Partnership Project (3GPP) network specifications, offers faster connectivity, lower latency, higher bit rates, and improved network reliability. This technology is crucial to support critical applications such as the Internet of Things (IoT) and industrial use cases targeting pivotal infrastructures [1], [2]. However, several components and interfaces of the Next-Generation Radio Access Network (NG-RAN) and the 5G core itself are vulnerable to attacks, which can potentially disrupt end-to-end communication services.

While a particular emphasis has been given to the security of NG-RAN, there are not many studies investigating the security issues of the 5G core. In this paper, we focus on the security issues of the Packet Forwarding Control Protocol (PFCP) protocol, which is utilised in the N4 interface between the Session Management Function (SMF) and the User Plane Function (UPF) in the 5G core. In particular, based on the PFCP attacks investigated in our previous work in [3], in this paper, we introduce a labelled intrusion detection dataset, called *5GC PFCP Intrusion Detection Dataset*, which was generated in the context of the *H2020 SANCUS* project, a collaborative research initiative funded by the European Union (EU) to enhance the security of 5G networks. This security dataset can fully support the development of Artificial Intelligence (AI)-powered Intrusion Detection and Prevention Systems (IDPS) against these attacks.

The proposed dataset is available in IEEE Dataport and Zenodo and can support the development of IDPS that adopt Machine Learning (ML) and Deep Learning (DL) methods. We construct this dataset by following the methodological framework of A. Gharib et al. [4]. Therefore, our dataset is characterised by eleven main attributes: (a) Complete Network Configuration, (b) Complete Traffic, (c) Labelled Dataset, (d) Complete Interaction, (e) Complete Capture, (f) Available Protocols, (g) Attack Diversity, (h) Heterogeneity, (i) Feature Set and (j) Metadata. Therefore, the contributions of this paper are summarised as follows:

- **5G Core Testbed and PFCP Attacks**: A virtualised 5G environment was implemented in order to investigate PFCP attacks against the 5G core. Four PFCP-related attacks are examined, targeting the communication between SMF and UPF.
- **5GC PFCP Intrusion Detection Dataset**: Based on the previous PFCP attacks, a new labelled security dataset is implemented and shared publicly in order to support the development of AI solutions for intrusion detection. This dataset is available in IEEE Dataport[1] and Zenodo [2].

Based on the previous remarks, the rest of this paper is organised as follows. Section II discusses the 5G testbed and

*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement 952672 (SANCUS).

† G. Amponis, P. Radoglou-Grammatikis and G. Nakas are with K3Y Ltd. Sofia 1612, Bulgaria - E-Mail: {gamponis, pradoglou, gnakas}@k3y.bg

‡ G. Amponis and T. Lagkas are with the Department of Computer Science, International Hellenic University, Kavala Campus, 65404, Greece - E-Mail: {geaboni, tlagkas}@cs.ihu.gr

§ P. Radoglou Grammatikis and P. Sarigiannidis are with the Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani 50100, Greece - E-Mail: {pradoglou, psarigiannidis}@uowm.gr

¶ Sotirios Goudos is with the Department of Physics, Aristotle University of Thessaloniki, Thessaloniki, 54124, Greece - E-Mail: {sgoudo}@physics.auth.gr

‖ V. Argyriou is with the Department of Networks and Digital Media, Kingston University London, Penrhyn Road, Kingston upon Thames, Surrey KT1 2EE, UK - E-Mail: vasileios.argyriou@kingston.ac.uk

[1]https://ieee-dataport.org/documents/5gc-pfcp-intrusion-detection-dataset-0

[2]https://zenodo.org/record/7888347#.ZFejbNJBxhE

the relevant attacks used to compose the 5GC PFCP Intrusion Detection Dataset. Section III provides the structure of the dataset. Section IV summarises the features and the balanced files that can be utilised by ML and DL methods. Finally, section V gives the concluding remarks of the paper.

II. 5G Testbed and PFCP Attacks

As depicted in Fig. 1, an experimental 5G testbed was used to develop the 5GC PFCP Intrusion Detection Dataset, including the following 5G network functions: Network Slice Selection Function (NSSF), the Network Exposure Function (NEF), the Network Repository Function (NRF), the Policy Control Function (PCF), the User Data Management (UDM), the Access and Mobility Management Function (AF), the Authentication Server Function (AUSF), the Access Management Function (AMF), SMF and UPF. Moreover, a virtualised UE, a virtualised gNodeB (gNb) and an attacker instance impersonating a maliciously instantiated SMF were used to generate the dataset. This testbed was implemented, utilising `Open5GS` as the cellular core [5], and `UERANSIM` as NG-RAN. Thus, the following PFCP attacks were emulated in a coordinated manner in order to construct the dataset.

PFCP Session Establishment DoS Attack: The aim of this attack is to exhaust the resources of the UPF by inundating it with genuine Session Establishment Requests and Heartbeat Requests. This could potentially hinder the 5G core's ability to create new Protocol Data Unit (PDU) sessions between clients and DN. The attack is executed on the N4 interface and could affect the intermediate interfaces as well. To evade detection, a unique Session ID (SEID) is generated for every session establishment request.

PFCP Session Deletion DoS Attack: The goal of this attack is to disconnect a specific UE from the DN. The script focuses on PDU sessions between clients and DN in such a way that only the DN is disconnected, while the UE remains connected to the NG-RAN or the Core network. The attack is executed on the N4 interface, and its impact is noticeable on the N6 interface. The only way to restore the connection of an affected UE is to re-initiate the session, either by restarting the session or entering the coverage area of another gNb. In such cases, a new SEID is assigned to the UE's PDU session, rendering the attack ineffective.

PFCP Session Modification Flood attack (DROP Apply Action Field Flags): The objective of this attack is to invalidate packet handling rules for a specific session, leading to the disassociation of a targeted UE from the DN. When successful, the Forwarding Action Rule (FAR) rules that contain the base station's Tunnel Endpoint Identifier (TEID) and IP address are removed from the UPF. This action cuts off the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) tunnel for the subscriber's downlink data, depriving them of internet connectivity. However, the GPRS Tunneling Protocol - User Plane (GTP-U) tunnel can be restored by transmitting the necessary data to the UPF. Similar to other PFCP-based attacks, this script focuses on the PDU sessions between the clients and the DN in such a way that only the DN is disconnected, and the UE remains connected to the 5G RAN or the Core network. The attack is executed on the N4 interface and may affect the N6 interface.

PFCP Session Modification Flood attack (DUPL Apply Action Field Flag): The aim of this attack is to utilise the `DUPL` flag in the Apply Action field to compel the UPF to replicate rules for the session, generating multiple paths for the same data from a single source. This can result in undefined behaviour in the N6 interface and/or cause traffic to be duplicated during transmission to the DN. Additionally, this attack may be part of a larger scheme to carry out a Distributed Denial of Service (DDoS) attack against hosts within the DN, while also overwhelming the UPF's resources to forward outgoing packets to external hosts outside the 5G core. By amplifying the number of transmitted packets per active user, a malicious entity can create an almost passive attack vector that can be effortlessly scaled to impact the traffic of numerous subscribers, exponentially draining the packet handling resources of the UPF.

The attacks were performed in the following order: First, on Wednesday, October 5, 2022, the PFCP Session Establishment DoS Attack was performed for four hours. Continuing, on Thursday, October 13, 2022, the PFCP Session Deletion DoS Attack was performed for four hours. Then, on Tuesday, November 01, 2022, the PFCP Session Modification DoS Attack with the `DROP` flag was performed for four hours. Finally, on Tuesday, November 22, 2022, the PFCP Session Modification DoS Attack with a `DUPL` flag in the Apply Action Field Flag was performed for four hours.

III. Dataset Structure

The previous PFCP attacks were carried out using security tools, such as `scapy`,`pcap-splitter`, `editcap` and `CICFlowMeter`. Each attack is provided by a 7z/zip file that contains the network traffic and flow statistics for each entity involved. Specifically, each 7z/zip file includes (a) pcap files for each entity, (b) Transmission Control Protocol (TCP)/Internet Protocol (IP) network flow statistics in a Comma-Separated Values (CSV) format, and (c) PFCP flow statistics for each entity, utilising different timeout values (such as 15, 20, 60, 120, and 240 seconds). The TCP/IP network flow statistics were generated using `CICFlowMeter`, while the PFCP flow statistics were produced using a `Custom PFCP Flow Generator`.

Based on the aforementioned remarks, the dataset consists of the following 7z/zip files:

- **Balanced PFCP APP Layer.7z/zip**: It includes the balanced CSV files from CICFlowMeter that may be used to train ML and DL algorithms. Each folder includes a different subfolder for the corresponding flow timeout values used by the Custom PFCP Flow Generator.
- **Balanced TCP-IP Layer.7z/zip**: It includes the balanced CSV files from the Custom PFCP Flow Generator that may be used to train ML and DL algorithms. Each folder includes a different sub-folder for the corresponding flow timeout values used by CICFlowMeter.

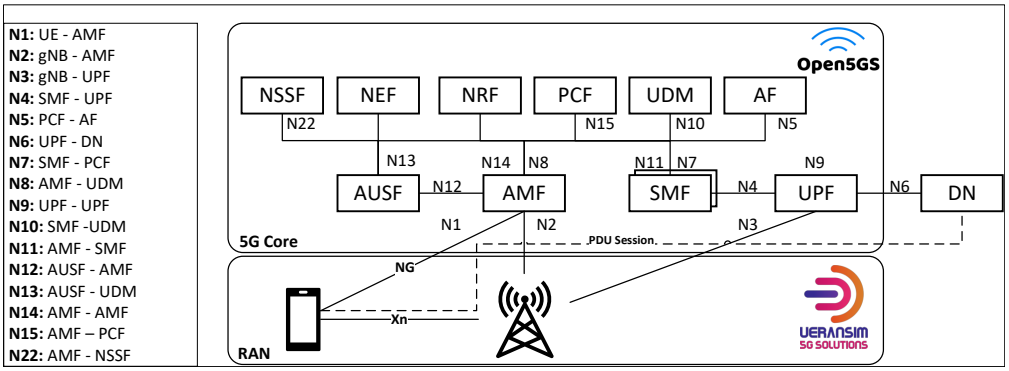

Figure 1. 5G Testbed used to generate 5GC PFCP Intrusion Detection Dataset

- **PFCP Session Deletion DoS Attack.7z/zip**: It includes the pcap files and CSV files related to the PFCP Session Deletion Denial of Service (DoS) Attack.
- **PFCP Session Establishment DoS Attack.7z/zip**: It includes the pcap files and CSV files related to the PFCP Session Establishment Flood DoS Attack.
- **PFCP Session Modification DoS Attack.7z/zip**: It includes the pcap files and CSV files related to the PFCP Session Modification DoS Attack.

IV. Features and Balanced Files

Table I
Application Layer PFCP Flow Statistics – Features

Feature	Description
flow ID	Flow identifier
source IP	Source IP address
destination IP	Destination IP address
source port	Source port number
destination port	Destination port number
protocol	Network layer protocol
duration	Length of time flow was active
fwd_packets	Number of forward packets
bwd_packets	Number of backward packets
PFCPHeartbeatRequest_counter	Number of PFCP Heartbeat Request messages
PFCPHeartbeatResponse_counter	Number of PFCP Heartbeat Response messages
PFCPPFDManagementRequest_counter	Number of PFCP PFD Management Request messages
PFCPPFDManagementResponse_counter	Number of PFCP PFD Management Response messages
PFCPAssociationSetupRequest_counter	Number of PFCP Association Setup Request messages
PFCPAssociationSetupResponse_counter	Number of PFCP Association Setup Response messages
PFCPAssociationUpdateRequest_counter	Number of PFCP Association Update Request messages
PFCPAssociationUpdateResponse_counter	Number of PFCP Association Update Response messages
PFCPAssociationReleaseRequest_counter	Number of PFCP Association Release Request messages
PFCPAssociationReleaseResponse_counter	Number of PFCP Association Release Response messages
PFCPVersionNotSupportedResponse_counter	Number of PFCP Version Not Supported Response messages
PFCPNodeReportRequest_counter	Number of PFCP Node Report Request messages
PFCPNodeReportResponse_counter	Number of PFCP Node Report Response messages
PFCPSessionSetDeletionRequest_counter	Number of PFCP Session Set Deletion Request messages
PFCPSessionSetDeletionResponse_counter	Number of PFCP Session Set Deletion Response messages
PFCPSessionEstablishmentRequest_counter	Number of PFCP Session Establishment Request messages
PFCPSessionEstablishmentResponse_counter	Number of PFCP Session Establishment Response messages
PFCPSessionModificationRequest_counter	Number of PFCP Session Modification Request messages
PFCPSessionModificationResponse_counter	Number of PFCP Session Modification Response messages
PFCPSessionDeletionRequest_counter	Number of PFCP Session Deletion Request messages
PFCPSessionDeletionResponse_counter	Number of PFCP Session Deletion Response messages
PFCPSessionReportRequest_counter	Number of PFCP Session Report Request messages
PFCPSessionReportResponse_counter	Number of PFCP Session Report Response messages
Downlink_counter	Number of downlink packets
Uplink_counter	Number of uplink packets
Bidirectional_traffic_counter	Number of bidirectional traffic packets
Label	Flow label (e.g. benign or malicious)

Two balanced versions of the dataset have been created for the TCP/IP flow statistics generated by `CICFlowMeter` (Table II) and the PFCP flow statistics produced by the `Custom PFCP Flow Generator` (Table I). Each version is balanced. Therefore, they contain an equal number of samples for each of the classes. The five classes and their labels are available in Table III. The two balanced versions are summarised by the files `Balanced_PFCP_APP_Layer.7z/zip` and `Balanced_TCP-IP_Layer.7z/zip`. The first file contains the PFCP flow statistics, while the second file includes the TCP/IP flow statistics. Each file also contains a set of subfolders for each flow timeout value. In particular, five values were used: 15s, 20s, 60s, 120s, and 240s. In addition, there are two sub-subfolders, namely `Training` and `Testing`. Each of these sub-subfolders contains a .csv file named `Training_X.csv` and `Testing_X.csv`, where X is the flow timeout value. The split ratio is: 70% - 30%, for the training and testing processes, respectively. In addition, the splitting is stratified, meaning that the same percentage of samples of each class are present in each training and testing dataset. The number of flows per each flow timeout value for `Balanced_TCP-IP_Layer.7z/zip` are presented in Table IV, while the number of flows for each flow timeout value for `Balanced_PFCP_APP_Layer.7z/zip` are provided in Table V.

V. Conclusions

The communication points in the 5G core can lead to various security weaknesses that are investigated by both academia and industry. In this paper, we present the *5GC PFCP Intrusion Detection Dataset*, which was generated in the context of the H2020 SANCUS project. This security dataset is publicly available in IEEE Dataport and Zenodo and can be utilised for the development of AI-powered intrusion detection and prevention mechanisms. It includes the network traffic data (i.e., pcap files) and labelled TCP/IP and PFCP flow statistics related to four PFCP cyberattacks, namely (a) PFCP Session Establishment DoS Attack, (b) PFCP Session Deletion DoS Attack, (c) PFCP Session Modification Flood attack (DROP Apply Action Field Flags) and (d) PFCP Session Modification Flood attack (DUPL Apply Action Field Flag).

References

[1] P. Radoglou-Grammatikis, P. Sarigiannidis, C. Dalamagkas, Y. Spyridis, T. Lagkas, G. Efstathopoulos, A. Sesis, I. L. Pavon, R. T. Burgos, R. Diaz, A. Sarigiannidis, D. Papamartzivanos, S. A. Menesidou, G. Ledakis, A. Pasias, T. Kotsiopoulos, A. Drosou, O. Mavropoulos,

Table II
TCP/IP NETWORK FLOW STATISTICS - FEATURES

Feature	Description
Flow ID	ID of the flow
Src IP	Source IP address
Src Port	Source TCP/UDP port
Dst IP	Destination IP address
Dst Port	Destination TCP/UDP port
Protocol	Protocol related to the flow
Timestamp	Flow timestamp
Flow Duration	Duration of the flow in Microseconds
Tot Fwd Pkts	Total packets in forward direction
Tot Bwd Pkts	Total packets in backward direction
TotLen Fwd Pkts	Total size of packets in forward direction
TotLen Bwd Pkts	Total size of packets in backward direction
Fwd Pkt Len Max	Maximum size of packet in forward direction
Fwd Pkt Len Min	Minimum size of packet in forward direction
Fwd Pkt Len Mean	Mean size of packet in forward direction
Fwd Pkt Len Std	Standard deviation size of packet in forward direction
Bwd Pkt Len Max	Maximum size of packet in backward direction
Bwd Pkt Len Min	Minimum size of packet in backward direction
Bwd Pkt Len Mean	Mean size of packet in backward direction
Bwd Pkt Len Std	Standard deviation size of packet in backward direction
Flow Byts/s	Number of flow bytes per second
Flow Pkts/s	Number of flow packets per second
Flow IAT Mean	Mean time between two packets sent in the flow
Flow IAT Std	Standard deviation time between two packets sent in the flow
Flow IAT Max	Maximum time between two packets sent in the flow
Flow IAT Min	Minimum time between two packets sent in the flow
Fwd IAT Tot	Total time between two packets sent in the forward direction
Fwd IAT Mean	Mean time between two packets sent in the forward direction
Fwd IAT Std	Standard deviation time between two packets sent in the forward direction
Fwd IAT Max	Maximum time between two packets sent in the forward direction
Fwd IAT Min	Minimum time between two packets sent in the forward direction
Bwd IAT Tot	Total time between two packets sent in the backward direction
Bwd IAT Mean	Mean time between two packets sent in the backward direction
Bwd IAT Std	Standard deviation time between two packets sent in the backward direction
Bwd IAT Max	Maximum time between two packets sent in the backward direction
Bwd IAT Min	Minimum time between two packets sent in the backward direction
Fwd PSH Flags	Number of Forward PSH flags
Bwd PSH Flags	Number of Backward PSH flags
Fwd URG Flags	Number of Forward URG flags
Bwd URG Flags	Number of Backward URG flags
Fwd Header Len	Length of Forward header
Bwd Header Len	Length of Backward header
Fwd Pkts/s	Number of Forward packets per second
Bwd Pkts/s	Number of Backward packets per second
Pkt Len Min	Minimum packet length
Pkt Len Max	Maximum packet length
Pkt Len Mean	Mean packet length
Pkt Len Std	Standard deviation of packet length
Pkt Len Var	Variance of packet length
FIN Flag Cnt	Number of FIN flags
SYN Flag Cnt	Number of SYN flags
RST Flag Cnt	Number of RST flags
PSH Flag Cnt	Number of PSH flags
ACK Flag Cnt	Number of ACK flags
URG Flag Cnt	Number of URG flags
CWE Flag Count	Number of CWE flags
ECE Flag Cnt	Number of ECE flags
Down/Up Ratio	Down/Up ratio
Pkt Size Avg	Average packet size
Fwd Seg Size Avg	Average Forward segment size
Bwd Seg Size Avg	Average Backward segment size
Fwd Byts/b Avg	Average Forward bytes per bit
Fwd Pkts/b Avg	Average Forward packets per bit
Fwd Blk Rate Avg	Average Forward block rate
Bwd Byts/b Avg	Average Backward bytes per bit
Bwd Pkts/b Avg	Average Backward packets per bit
Bwd Blk Rate Avg	Average Backward block rate
Subflow Fwd Pkts	Number of Forward subflow packets
Subflow Fwd Byts	Number of Forward subflow bytes
Subflow Bwd Pkts	Number of Backward subflow packets
Subflow Bwd Byts	Number of Backward subflow bytes
Init Fwd Win Byts	Initial Forward window bytes
Init Bwd Win Byts	Initial Backward window bytes
Fwd Act Data Pkts	Number of Forward active data packets
Fwd Seg Size Min	Minimum Forward segment size
Active Mean	Mean active time
Active Std	Standard deviation of active time
Active Max	Maximum active time
Active Min	Minimum active time
Idle Mean	Mean idle time
Idle Std	Standard deviation of idle time
Idle Max	Maximum idle time
Idle Min	Minimum idle time
Label	Label

Table III
CLASSES OF THE 5GC PFCP INTRUSION DETECTION DATASET

Class	Label
Normal flow	Normal
PFCP Session Establishment Flood attack flow	Mal_Estab
PFCP Session Deletion Flood attack flow	Mal_Del
PFCP Session Modification Flood attack (DROP Apply Action Field Flags) flow	Mal_Mod
PFCP Session Modification Flood attack (DUPL Apply Action Field Flag) flow	Mal_Mod2

Table IV
NUMBER OF THE TCP/IP FLOWS (GENERATED BY CICFLOWMETER) FOR THE DIFFERENT FLOW TIMEOUT VALUES IN THE BALANCED FILES

Training					
Timeout	**Normal**	**Mal_Estab**	**Mal_Del**	**Mal_Mod**	**Mal_Mod2**
15s	1439	1440	1440	1440	1440
20s	1439	1440	1440	1440	1440
60s	485	485	485	485	485
120s	260	261	260	260	261
240s	133	134	133	134	134
Testing					
Timeout	**Normal**	**Mal_Estab**	**Mal_Del**	**Mal_Mod**	**Mal_Mod2**
15s	618	617	617	617	617
20s	618	617	617	617	617
60s	208	208	208	208	208
120s	112	111	112	112	111
240s	58	57	58	57	57

Table V
NUMBER OF THE PFCP FLOWS (GENERATED BY CUSTOM PFCP FLOW GENERATOR) FOR THE DIFFERENT FLOW TIMEOUT VALUES IN THE BALANCED FILES

Training					
Timeout	**Normal**	**Mal_Estab**	**Mal_Del**	**Mal_Mod**	**Mal_Mod2**
15s	1103	1104	1104	1104	1104
20s	666	667	666	666	667
60s	222	223	222	223	223
120s	110	111	110	111	111
240s	68	69	68	69	69
Testing					
Timeout	**Normal**	**Mal_Estab**	**Mal_Del**	**Mal_Mod**	**Mal_Mod2**
15s	474	473	473	473	473
20s	286	285	286	286	285
60s	96	95	96	95	95
120s	48	47	48	47	47
240s	30	29	30	29	29

A. C. Subirachs, P. P. Sola, J. L. Domínguez-García, M. Escalante, M. M. Alberto, B. Caracuel, F. Ramos, V. Gkioulos, S. Katsikas, H. C. Bolstad, D.-E. Archer, N. Paunovic, R. Gallart, T. Rokkas, and A. Arce, "SDN-Based Resilient Smart Grid: The SDN-microSENSE Architecture," *Digital*, vol. 1, no. 4, pp. 173–187, 2021. [Online]. Available: https://www.mdpi.com/2673-6470/1/4/13

[2] 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)*, 2022, pp. 1–4.

[3] G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, W. Mallouli, A. Cavalli, D. Klonidis, E. Markakis, and P. Sarigiannidis, "Threatening the 5g core via pfcp dos attacks: the case of blocking uav communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 124, Dec 2022. [Online]. Available: https://doi.org/10.1186/s13638-022-02204-5

[4] A. Gharib, I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "An evaluation framework for intrusion detection dataset," in *2016 International Conference on Information Science and Security (ICISS)*. IEEE, 2016, pp. 1–6.

[5] P. Kiri Taksande, P. Jha, A. Karandikar, and P. Chaporkar, "Open5G: A Software-Defined Networking Protocol for 5G Multi-RAT Wireless Networks," in *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2020, pp. 1–6.