5G-Fuzz An Attack Generator for Fuzzing 5GC, using Generative Adversarial Networks

G. Nakas, P. Radoglou-Grammatikis, G. Amponis, T. Lagkas, V. Argyriou, S.Goudos , P. Sarigiannidis

SANCUS

Authors

George Nakas, Panagiotis Radoglou-Grammatikis, George Amponis
Research and Development Department
K3Y Ltd., Bulgaria
{gnakas, pradoglou, gamponis}@k3y.bg

Thomas Lagkas
Department of Computer Science, International Hellenic University, Greece
tlagkas@cs.ihu.gr

Vasileios Argyriou
Department of Networks and Digital Media
Kingston University, United Kingdom
vasileios.argyriou@kingston.ac.uk

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

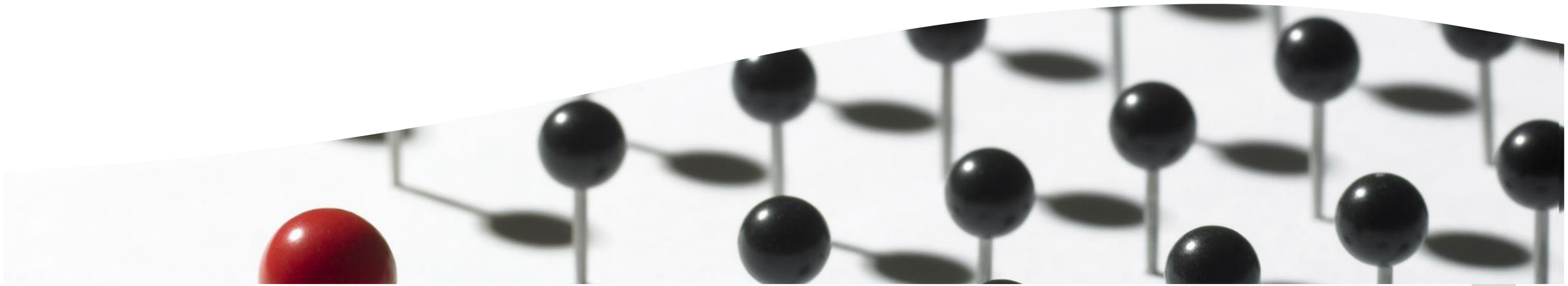
Panagiotis Radoglou-Grammatikis, Panagiotis Sarigiannidis
Department of Electrical and Computer Engineering
University of Western Macedonia, Greece
{pradoglou, psarigiannidis}@uowm.gr

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 952672 (SANCUS).

Outline

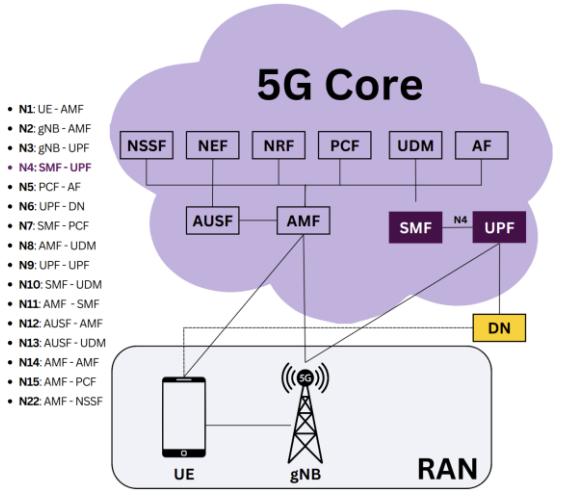
- Motivation
- Attack Modelling
- Design & Implementation
- Evaluation
- Conclusion

Motivation



Motivation[1/2] – Introduction

- The evolution of **5G** networks represents a significant technological leap towards a seamless and advanced user experience.
- Despite the advantages of 5GC, its **distributed** and **complicated** architecture creates an increased **attack surface**, where cyberattackers may exploit potential security weaknesses and take control of NFs
- Conventional fuzzing techniques generate random or brute-force data in order to test the target system.
- In contrast to conventional fuzzers, **5G-Fuzz** adopts two GANs in order to identify and generate the appropriate values of **SEID** and **seq** utilised in the PFCP sessions, thus accelerating the PFCP attacks.



Motivation[2/2] – Aim of this work

A smart fuzzer called **5G-FUZZ**, which targets the **PFCP** communications between **SMF** and **UPF** in 5GC. In particular, the proposed fuzzer takes full advantage of existing PFCP-related cyberattacks and adopts two **Generative Adversarial Networks (GANs)** in order to compose a combination of malicious PFCP traffic data that will next be redirected to UPF.

The main contributions include:

- **Implementation of a Smart Fuzzer for 5GC**: A smart fuzzer is provided, targeting the PFCP communications in 5GC. Therefore, PFCP-related vulnerabilities can be discovered and remediated in the context of particular 5GC instances.

- **Generating Malicious Network Traffic Data:** The proposed fuzzer can synthesise and generate malicious PFCP traffic data (i.e., pcap files) that next can be further processed and used to train ML and DL models for intrusion detection.

Attack Modelling

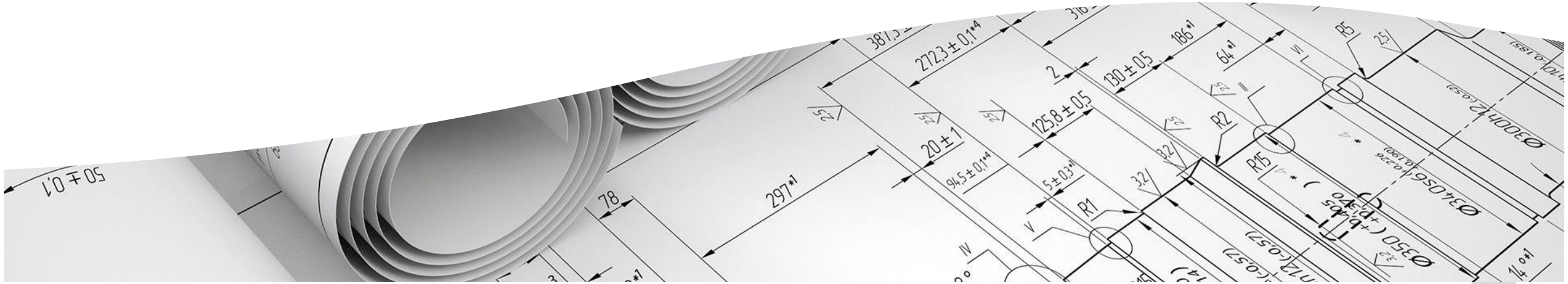
Attack Modelling

5G-Fuzz targets the N4 interface of 5GC between UPF and SMF. For this interface, PFCP is used. We focus our attention on the following PFCP-related attacks:

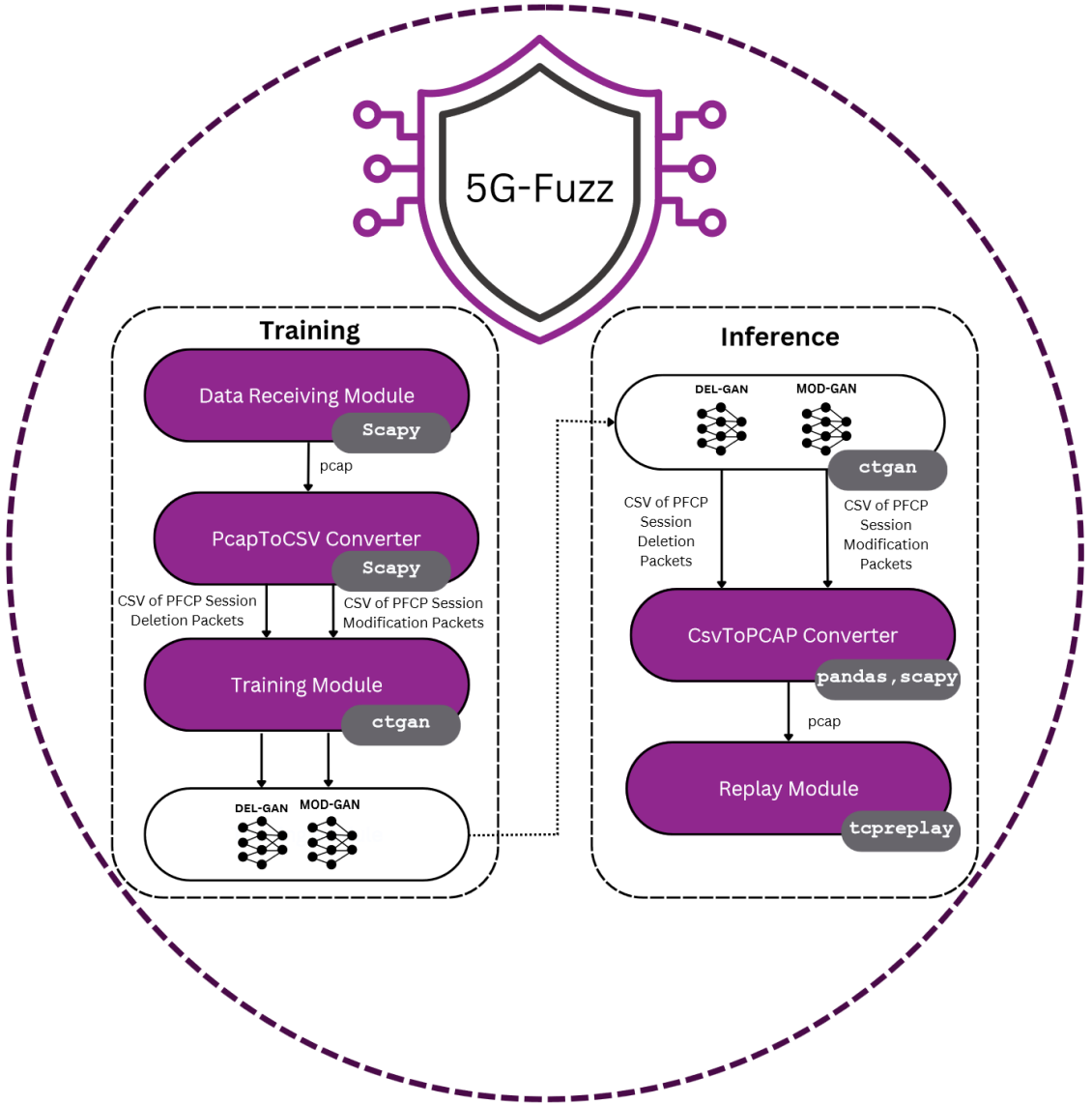
- **PFCP Session Deletion DoS Attack:** The goal of this cyberattack is to drop the connection between a User Equipment (UE) and the Data Network (DN). More specifically, the Python script behind this cyberattack disrupts the sessions between the UE and DN's Protocol Data Units (PDUs) without disconnecting the UE from the 5G Radio Access Network (RAN) or 5GC.
- **PFCP Session Modification DoS Attack (DROP):** The goal of this attack is to remove the packet-handling rules of a specific session between SMF and UPF. In particular, the cyberattacker, intends to remove the entries of the Forwarding Action Rules (FAR) that are associated with the Tunnel Endpoint Identifier (TEID) and the gNB IP address.

Although these cyberattacks are efficient by themselves, an attacker without prior knowledge about the target 5GC may require a lot of time for the identification of the appropriate SEID. Therefore, the goal of **5G-Fuzz** is to fully leverage historical data in order to generate similar, malicious data related to the parameters of the previous PFCP attacks. More specifically, **5G-Fuzz** focuses on the **seid** and **seq** fields of the PFCP Session Deletion Request and PFCP Session Modification Request packets.

Design & Implementation

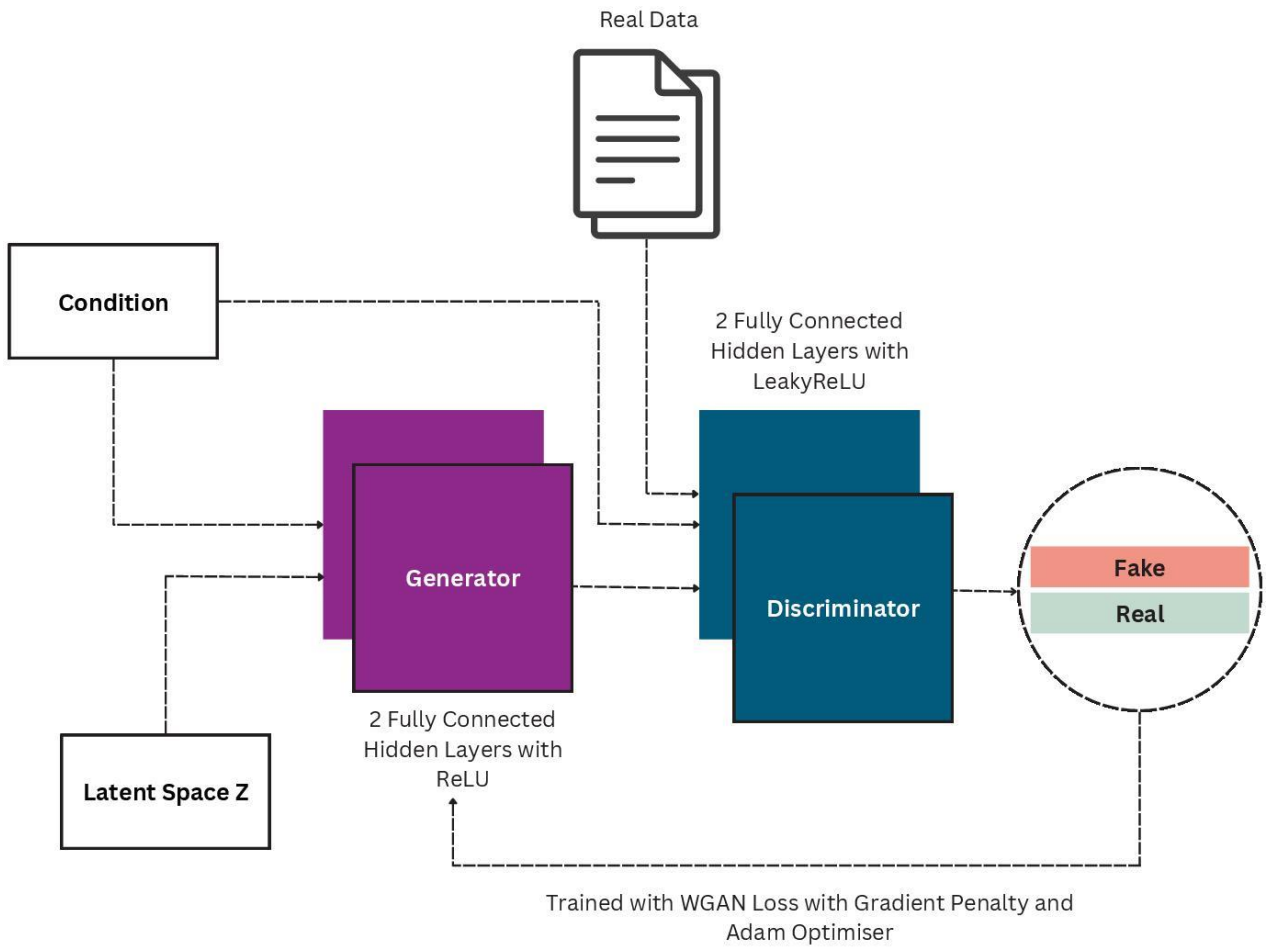


Methodology – 5G-Fuzz Architecture



Methodology – CTGAN Architecture

For the implementation of the DEL-GAN and the MOD-GAN, the CTGAN architecture is utilized:



Evaluation

Evaluation[1/3] – Evaluation Data

- For the evaluation of **5G-FUZZ**, the *5GC Intrusion Detection Dataset* is used, while also a set of metrics has been defined, that evaluates the synthetic data compared to the real ones. The metrics are calculated for both the outputs of the **DEL-GAN** and **MOD-GAN**. In particular, the following metrics are used:

Features with discrete values	Features with continuous values
Total Variation Distance	Inverted Kolmogorov–Smirnov
Chi-Squared Test	Pearson's correlation coefficien
Category Coverage	Statistic Similarity
Discrete Kullback–Leibler divergenc	Continuous Kullback–Leibler divergence

Evaluation[2/3] – DEL-GAN Evaluation

Discrete Features				
Metric	Value	Min	Max	Goal
TVD	1	0	1	Maximize
Chi-Squared	1	0	1	Maximize
CatCov	1	0	1	Maximize
D-KLD	1	0	1	Maximize
Continuous Features				
Metric	Value	Min	Max	Goal
IKS	0.98	0	1	Maximize
PCC	0.99	-1	1	Maximize
StatS	0.97	0	1	Maximize
C-KLD	0.98	0	1	Maximize

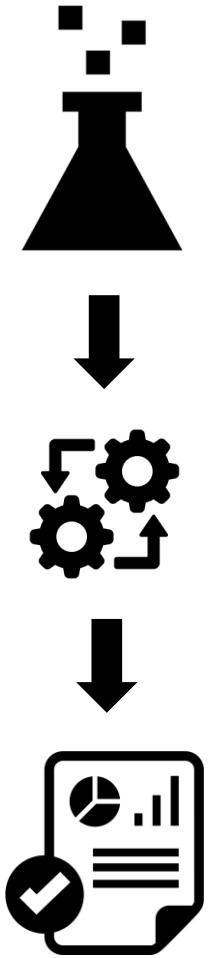
Evaluation[3/3] – MOD-GAN Evaluation

Discrete Features				
Metric	Value	Min	Max	Goal
TVD	1	0	1	Maximize
Chi-Squared	1	0	1	Maximize
CatCov	1	0	1	Maximize
D-KLD	1	0	1	Maximize
Continuous Features				
Metric	Value	Min	Max	Goal
IKS	0.99	0	1	Maximize
PCC	1	-1	1	Maximize
StatS	0.91	0	1	Maximize
C-KLD	0.99	0	1	Maximize

Conclusions

Conclusions

- Despite the advantages of 5G, it also comes with significant **security** and **privacy** concerns.
- For this reason, we present **5G-Fuzz**, a smart fuzzer that leverages historical data to fuzz and target the PFCP communications between SMF and UPF of 5GC.
- Unlike conventional fuzzers, **5G-Fuzz** employs two **GANs** to identify and generate appropriate values for the **SEID** and **seq** used in the **PFCP** sessions, thereby accelerating the various PFCP attacks. Then, **5G-Fuzz** creates and replays malicious PFCP packets against UPF.
- The evaluation analysis demonstrates that the proposed **5G-Fuzz** can generate realistic synthetic PFCP data.



Thank you for your attention!

https://sancus-project.eu/

gamponis@k3y.bg