5G CORE PFCP INTRUSION DETECTION DATASET

George Amponis [1, 2], Panagiotis Radoglou-Grammatikis [1, 3], George Nakas [1],
Sotirios Goudos [4], Vasileios Argyriou [5], Thomas Lagkas [2], and Panagiotis Sarigiannidis [3]

1. K3Y Ltd. Sofia, 1000 Bulgaria
2. Department of Computer Science, International Hellenic University, Kavala Campus, 65404, Greece
3. Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani 50100, Greece
4. Department of Physics, Aristotle University of Thessaloniki, Thessaloniki, 54124, Greece
5. Department of Networks and Digital Media, Kingston University London, Penrhyn Road, Kingston upon Thames, Surrey KT1 2EE, UK

INTRODUCTION

"5GC PFCP Intrusion Detection Dataset":

- Labeled dataset for detecting PFCP cyberattacks in 5G core networks.
- Enables AI-based intrusion detection systems for addressing cybersecurity challenges in 5G environments.
- Includes network flow statistics and relevant traffic data.
- Facilitates the development and evaluation of AI-based intrusion detection systems for the 5G core.

OBJECTIVE

- Objective of the "5GC PFCP Intrusion Detection Dataset":
  - Introduce and provide access to the dataset.
  - Valuable resource for training and evaluating AI-based intrusion detection models.
  - Specifically focuses on PFCP-related cyberattacks in the 5G core.
  - Facilitates the development of effective intrusion detection systems for 5G networks.

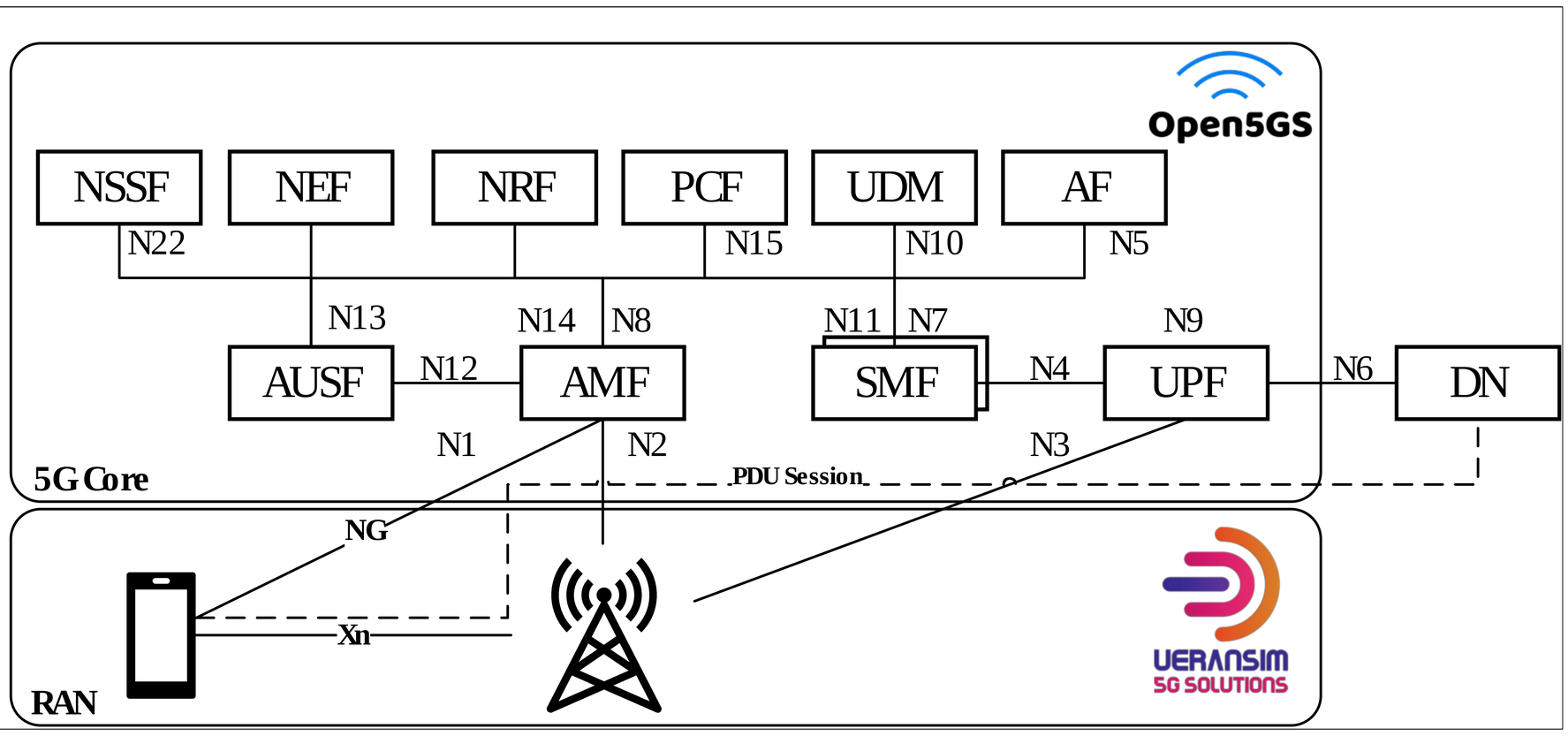
METHODOLOGY

- Investigation of PFCP attack scenarios:
  - Four specific PFCP attack scenarios were examined.
  - TCP/IP and application-layer statistics collected for dataset enrichment.
- Supervised learning:
  - Dataset is labeled to identify attack instances.
  - Enables the development of supervised learning-based intrusion detection models.
- Public availability:
  - Dataset can be accessed through IEEE Dataport and Zenodo repositories.

RESULTS

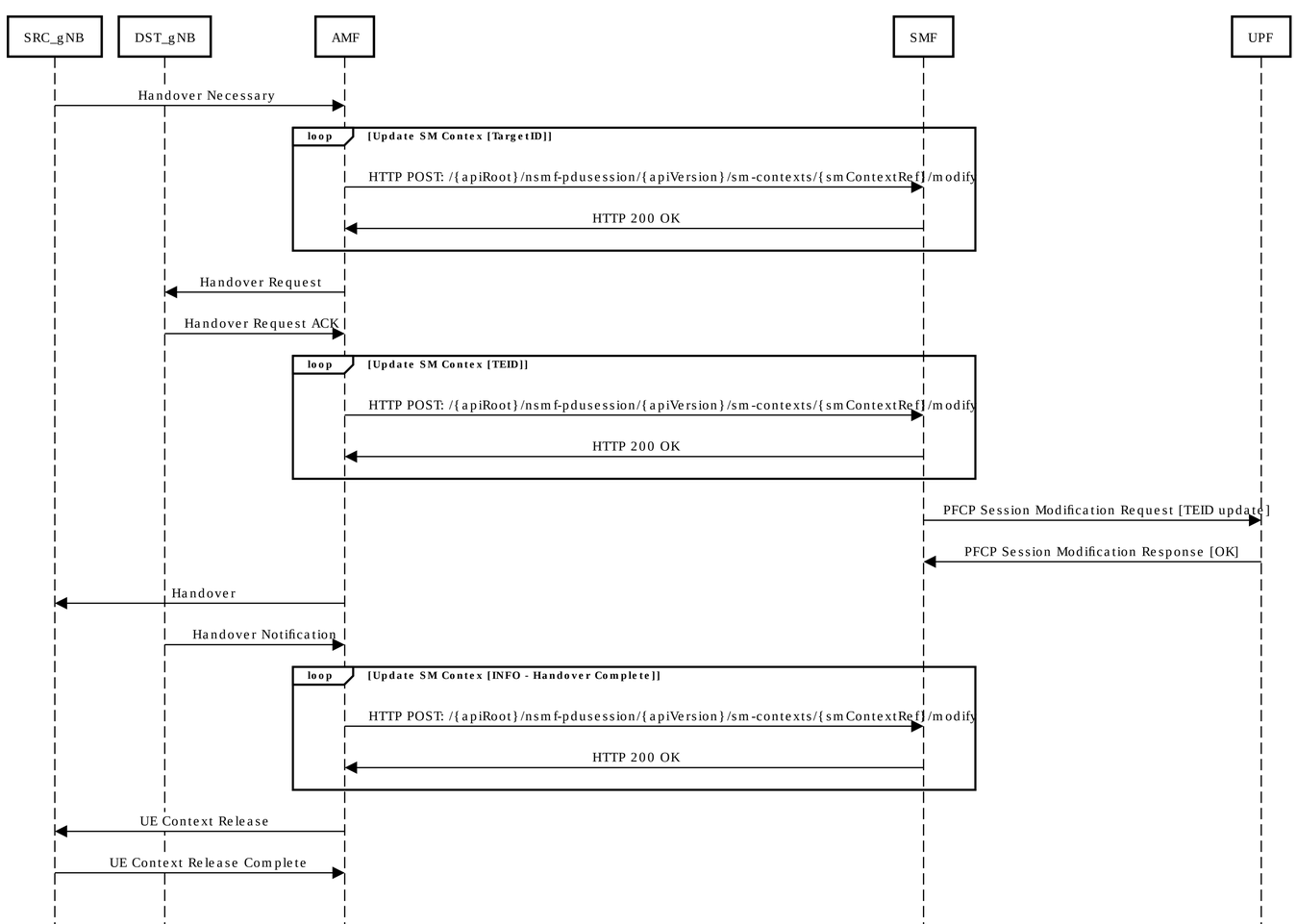
- Provision of f;ow statistics and traffic data for PFCP attacks in 5G core networks.
- AI intrusion detection development: Enables validation and benchmarking of AI intrusion detection models for 5G threats.
- Accessible through IEEE Dataport and Zenodo: Publicly available for easy access and collaboration.
- Advancement of intrusion detection in mobile core networks: We promote and advance intrusion detection in 5G mobile core networks.

N1: UE - AMF
N2: gNB - AMF
N3: gNB - UPF
N4: SMF - UPF
N5: PCF - AF
N6: UPF - DN
N7: SMF - PCF
N8: AMF - UDM
N9: UPF - UPF
N10: SMF -UDM
N11: AMF - SMF
N12: AUSF - AMF
N13: AUSF - UDM
N14: AMF - AMF
N15: AMF – PCF
N22: AMF - NSSF



ATTACK SCENARIOS

1. Session Establishment Flood
2. Session Deletion DoS Attack
3. Session Modification DoS Attack (DROP Flas)
4. Session Modification DoS Attack (DUPL Flag)



5G SIGNALLING AND PDU EFFECTS

N4 interface PFCP control signalling:

- Session Management Function (SMF)
- User Plane Function (UPF)

PDU Session Endpoints:

- User Equipment devices
- Data Network (through UPF)

Targeted Attributes:

- Session Endpoint Identifier (SEID)
- Tunnel Endpoint Identifier (TEID)

European Commission

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT 952672 (SANCUS).

SANCUS