dtec.bw

JAHRESTAGUNG 2024

Security in Private 5G Campus Networks

S.S. Ha[1], T.R. Doebbert[1], T. Kittel[2], M. Mieth[2], G.J. Scholl[1]
[1]Chair for Electrical Measurement Engineering, Helmut Schmidt University, Hamburg
[2]ipoque GmbH – A Rohde & Schwarz Company, Leipzig

Abstract

Modern manufacturing relies on a high degree of automation, where especially for functional safety applications hazards for humans and equipment must be prevented. Private 5G campus networks offer high flexibility, modularity, reduced installation and maintenance efforts. In modern communication systems, cybersecurity is of paramount importance, as emphasized by the Cyber Resilience Act (CRA). Therefore, a probing solution utilizing an AI-based deep packet inspection (DPI) is integrated within the private 5G environment, which is part of the "Digital Sensor-2-Cloud Campus Platform" (DS2CCP) [1] project, aiming to detect, e.g. potential anomalies in wireless communication between the industrial shop floor and the edge cloud. The goal is to provide a secure and functional safe test environment for safety applications being monitored and evaluated within the campus network. The AI-based deep packet inspection probing solution is part of a security strategy offering sovereignty within the network itself and deploying a digital twin of the communication traffic.

Scope

The communication traffic of the 5G campus network is monitored with the help of a probing solution using deep packet inspection generating transparency of the network traffic. The communication protocols (e.g., IIoT protocols such as OPC UA or MQTT) are verified and analyzed. In our case, especially functional safety protocols applying security-for-safety are communicated, verified and analyzed within the private 5G campus network. Therefore, the 5G network components and their communicated parameters are evaluated.
In an additional step, attack scenarios are identified and prepared for simulation. This is realized in hardware and simulated in software to easily integrate many user equipments (UEs) that perform attacks or are under attack. The attacks are detected using a probing solution with integrated deep packet inspection. Approaches for mitigation or attack prevention are developed. Classification and detection models are developed and evaluated with the help of AI techniques and a high performance cluster on campus (hpc.bw [9]).

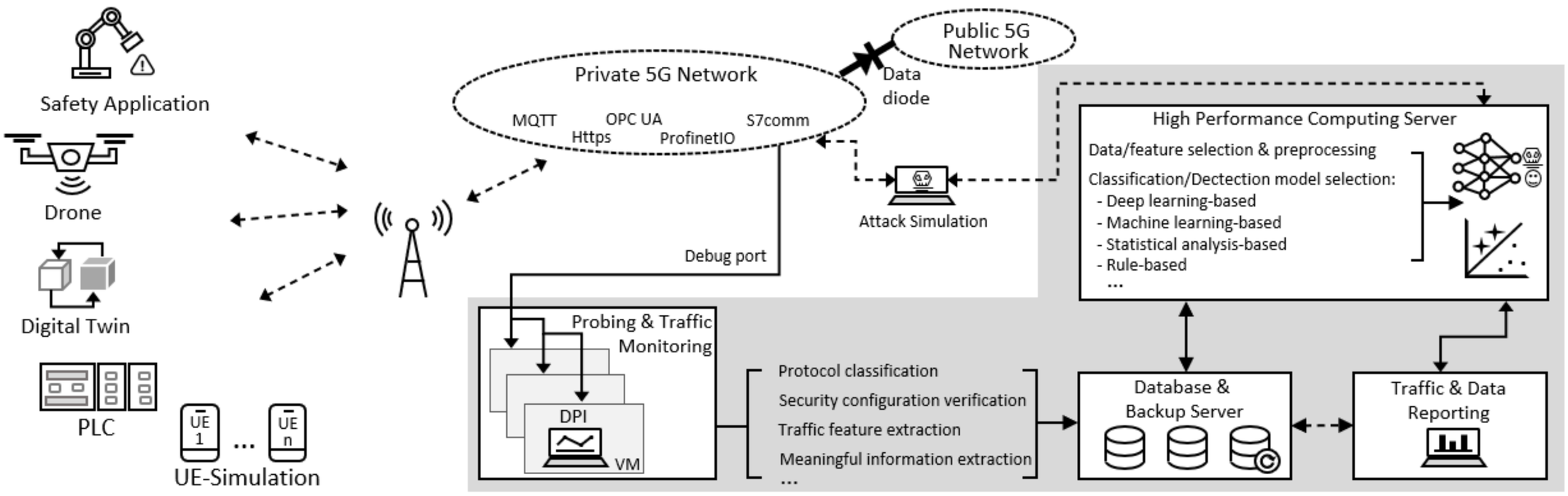

Fig. 1. AI-based DPI System of Industrial Wireless Environment Overview.

Architecture Setup

This work introduces a comprehensive end-to-end architecture designed to evaluate and enhance the security of private 5G environments, as shown in Fig.1. An industrial-grade probing solution using deep packet inspection is integrated within typical industrial safety applications. Additionally, AI techniques are utilized to achieve optimal system performance in detecting malicious behavior within the 5G network.
The summarized hardware components are as followed:

- Safety Application [2], Counter-UAS System [3], Siemens PLCs over 5G using Profinet/VxLAN protocol [4], UE-Simulation using UERANSIM [5].
- DPI: R&S®PACE 2 library [6] inside of a security probing and reporting solution.
- Private 5G Network: Ericsson Private 5G EP5G [7].
- The self-developed Data Diode for the separation of private and public networks [8].
- High Performance Computing for training AI model [9].
- Hardware Servers for simulation and abstraction.

References

[1] Helmut-Schmidt-University, "DS2CCP – Entwicklung einer digitalen Sensor-2-Cloud Campus-Plattform," dtec.bw Project website: http://dtecbw.de/home/forschung/hsu/project-ds2ccp.
[2] T. R. Doebbert, H. Beuster, G. Scholl, F. Fischer, and D. Merli, "Testbed for Functional Safety-Relevant Wireless Communication Based on IO-Link Wireless and 5G," (2022), dtec.bw-Beiträge der Helmut-Schmidt-Universität – Band 1, pp. 147-152.
[3] Wentzel, Alexander, Jan Cornils, and Marco Valentin. "Compact Counter-UAS System for Defeating Small UAV in Complex Environments", 9.-10. Okt. 2023, Copenhagen, Denmark.
[4] Siemens. "PROFINET communication in private industrial 5G networks," (2022), online available: https://assets.new.siemens.com/
[5] UERANSIM, online available: https://github.com/aligungr/UERANSIM
[6] R&S®PACE 2, Advanced protocol and application classification with metadata extraction for application-aware networking, online available: https://www.ipoque.com/products/
[7] Ericsson Private 5G EP5G, online available: https://www.ericssonlg.com/en/e-um-5g
[8] S. S. Ha, H. Beuster, T. R. Doebbert and G. Scholl, "An FPGA-based Unidirectional Gateway Proposal for OT-IT Network Separation to Secure Industrial Automation Systems," INDIN 2023, Lemgo, Germany, 2023, pp. 1-6.
[9] High Performance Computing, online available: https://www.hsu-hh.de/hpc/en/

unibw.de hsu-hh.de dtecbw.de

Digital Sensor-2-Cloud Campus-Platform

gefördert durch
dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr
Finanziert von der Europäischen Union
NextGenerationEU