

Security Monitoring of OPC UA over Industrial Private 5G Networks

S.S. Ha¹, F. Foerster², H. Beuster¹, K. Singh¹, E. Zeller¹, T. Kittel³, D. Merli², G. Scholl¹

¹Chair for Electrical Measurement Engineering, Helmut Schmidt University, Hamburg

²Institute for Innovative Safety and Security Technical University of Applied Sciences Augsburg

³ipoque GmbH – A Rohde & Schwarz Company, Leipzig

Motivation

Industrial private Fifth Generation (5G) networks enable flexible wireless communication for industrial applications, but realistic cybersecurity evaluation requires representative experimental environments and monitoring infrastructures [1]. Building on such an environment, machine learning (ML)-based intrusion detection systems (IDSs) have demonstrated that attacks against Open Platform Communications Unified Architecture (OPC UA) over industrial private 5G can be detected using traffic- and protocol-aware features [2].

When OPC UA uses SignAndEncrypt, payload inspection is no longer possible. Intrusion detection must therefore rely on residual transport, temporal, and protocol-lifecycle characteristics that remain observable in encrypted traffic [3]. However, benign 5G connectivity variations such as user equipment (UE) reconnections, Protocol Data Unit (PDU) session resets, and temporary interruptions can noticeably increase the false-positive rate (FPR), even in the absence of attacks [4].

These findings motivate future 5G control-plane (CP)-aware intrusion detection to improve IDS reliability under dynamic network conditions.

Research Objectives

- Develop and validate a representative industrial private 5G testbed that enables reproducible cybersecurity experiments with realistic OPC UA-based automation, heterogeneous endpoints, and network-side monitoring [1].
- Design and experimentally evaluate ML-based intrusion detection for OPC UA-specific attacks over industrial private 5G, using traffic-, flow-,

- and protocol-aware characteristics observable at the network level [2].
- Investigate attack detectability under OPC UA SignAndEncrypt and determine how residual transport, temporal, and protocol-lifecycle characteristics contribute to detecting malicious behavior when application payloads are no longer accessible [3].
- Assess IDS robustness under benign 5G connectivity variations and analyze how legitimate UE and PDU-session events influence false positives and their temporal relationship with CP activity [4].

Experimental Platform

- Experiments are conducted on an operational 3GPP Release 16 private 5G Standalone network with heterogeneous industrial endpoints and dedicated security monitoring [1].
- A representative OPC UA-based warehouse automation system integrates PLCs, HMIs, SCADA, engineering clients, and simulated industrial processes [2]–[4].
- The platform supports both unencrypted and SignAndEncrypt OPC UA communication; encrypted studies analyze mirrored user-plane (UP) traffic without payload decryption [2]–[3].
- The R&S@PACE 2 DPI engine extracts payload-independent traffic and OPC UA framing characteristics, aggregated into 5s time windows (TWs) for IDS processing.
- UE-level CP traces are collected separately and aligned with UP observations to analyze the relationship between 5G connectivity activity and IDS outputs [4].

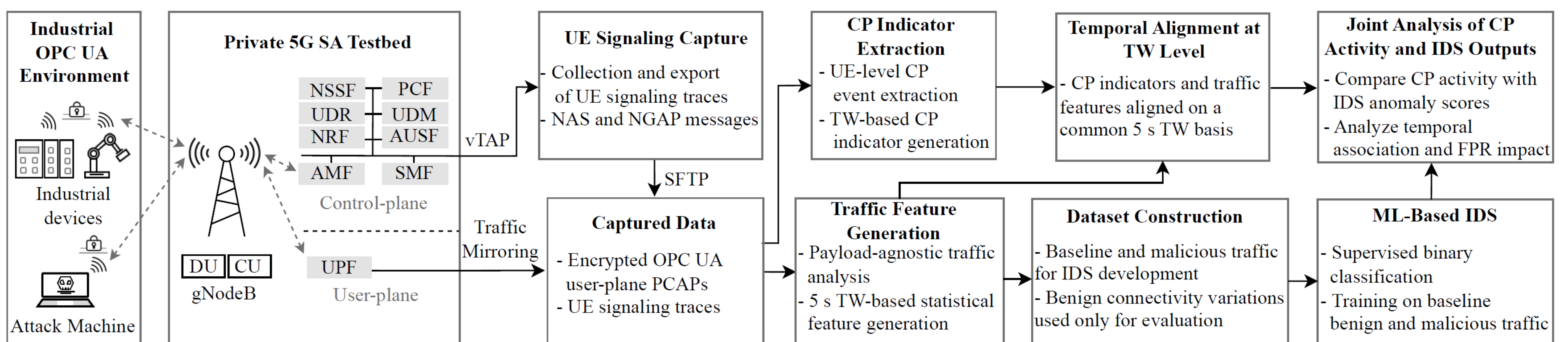


Fig. 1: Experimental Workflow for Encrypted OPC UA IDS Analysis with 5G CP Context

References

- [1] S. S. Ha, F. Foerster, T. R. Doebbert, T. Kittel, D. Merli, and G. Scholl. "Testbed and Software Architecture for Enhancing Security in Industrial Private 5G Networks". In: 2025 IEEE 30th International Conference on Emerging Technologies and Factory Automation (ETFA). 2025, pp. 1–4.
- [2] S. S. Ha, K. Singh, F. Foerster, H. Beuster, T. Kittel, D. Merli, and G. Scholl. "An Experimental Study of Machine Learning-Based Intrusion Detection for OPC UA over Industrial Private 5G Networks". In: 2026 IEEE 9th International Conference on Industrial Cyber-Physical Systems (ICPS). 2026, pp. 1–8.
- [3] S. S. Ha, F. Foerster, H. Beuster, E. Zeller, D. Merli, and G. Scholl. "Residual observability and attack detectability in encrypted OPC UA traffic". In: 2026 IEEE 52nd Annual Conference of the IEEE Industrial Electronics Society (IECON). in press. 2026.
- [4] S. S. Ha, F. Foerster, H. Beuster, T. Kittel, D. Merli, and G. Scholl. "Impact of benign connectivity variations on intrusion detection for encrypted OPC UA traffic in industrial private 5G networks". In: 2026 IEEE 31st International Conference on Emerging Technologies and Factory Automation (ETFA). in press. 2026.

Mehrwert für die Bundeswehr

The presented research could support the secure operation of future private 5G-based communication infrastructures in military environments, for example in logistics, maintenance, automation, and other networked technical systems. Network-based intrusion detection could provide additional security monitoring for encrypted OPC UA communication without requiring access to sensitive application payloads. The results also show that legitimate 5G connectivity procedures can influence IDS behavior and generate false alarms. Considering such network context could therefore help operators distinguish normal connectivity-related changes from potentially malicious activity. Overall, the findings provide a basis for more reliable cyber monitoring and situational awareness in future private 5G deployments in military environments.



unibw.de



hsu-hh.de



dtec.bw.de

gefördert durch



Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr



Finanziert von der Europäischen Union
NextGenerationEU