Simulation of IIoT-Driven Attack Vectors on 5G Core Networks: Dataset Generation and Machine Learning Based Detection

Suranga Prasad
Centre for Wireless Communications
University of Oulu
Oulu, Finland
Suranga.WengappuliArachchige@oulu.fi

Pramod Munaweera
Centre for Wireless Communications
University of Oulu
Oulu, Finland
pramod.munaweerakankanamge@oulu.fi

Tharaka Hewa
Centre for Wireless Communications
University of Oulu
Oulu, Finland
tharaka.hewa@oulu.fi

Yushan Siriwardhana
Centre for Wireless Communications
University of Oulu
Oulu, Finland
yushan.siriwardhana@oulu.fi

Mika Ylinattila
Centre for Wireless Communications
University of Oulu
Oulu, Finland
mika.ylinattila@oulu.fi

Abstract

The emergence of 5G technology has accelerated the development of Industrial Internet of Things (IIoT) applications, enabling a wide range of innovations across multiple industries. However, the integration of 5G and IIoT introduces new security vulnerabilities in core networks due to the vast number of connected devices and the lack of robust security measures in these devices. These vulnerabilities provide intruders with new opportunities to attack the core network. In our research, we demonstrate several types of potential attacks from IoT devices on the core network, collect the attack data into a proper dataset, and implement a Machine Learning (ML) model to detect these threats. The collected data can be used to test different ML models designed to detect intrusions in the core network. The results of this work will contribute to the development of advanced security measures, enhancing the resilience and reliability of 5G infrastructures against emerging cyber threats.

Keywords

5G Core, Security, IIoT, Attack, Dataset, Machine Learning

ACM Reference Format:
Suranga Prasad, Pramod Munaweera, Tharaka Hewa, Yushan Siriwardhana, and Mika Ylinattila. 2024. Simulation of IIoT-Driven Attack Vectors on 5G Core Networks: Dataset Generation and Machine Learning Based Detection. In *14th International Conference on the Internet of Things (IoT 2024), November 19–22, 2024, Oulu, Finland.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3703790.3703815

1 Introduction

5G technology offers faster speeds, lower latency, and greater capacity than previous versions [6]. This enhanced connectivity is crucial for the IIoT, which relies on 5G to connect and manage industrial devices, enabling smarter factories and real-time data analysis. With 5G's robust communication capabilities, IIoT applications are transforming industrial processes across various sectors [17][18].

However, IIoT devices are vulnerable to attacks due to factors like weak security measures, such as default passwords and inadequate encryption. Many IIoT devices lack advanced security features and suffer from poor management, including infrequent updates or reliance on outdated hardware. The scale and diversity of IIoT devices create a large attack surface, worsened by less secure communication protocols and limited device resources that can't support complex security software. Additionally, physical vulnerabilities, weak authentication, and supply chain issues increase the risk of breaches in IIoT systems [7][11]. Real-world attacks like Stuxnet [4], the Ukraine power grid hack [3], the Mirai Botnet [1], and Triton malware [5] reveal significant vulnerabilities in IIoT systems, particularly in critical infrastructure.

An attack on the 5G core network can severely impact various industries due to its central role in managing essential network functions [6]. For instance, a breach might disrupt critical communications in healthcare, affecting remote surgeries or emergency services, and could also halt industrial operations by stopping production lines or disabling safety systems in factories. Since the 5G core is central to many services, securing it against threats from IIoT devices and other attack vectors is crucial to maintain operational integrity.

Recent research has focused on enhancing 5G security, particularly against DDoS attacks, through ML techniques. One study [10] integrates intelligent Intrusion Detection Systems (IDSs) into 5G networks, using ML to detect and mitigate new threats more effectively, reducing false alarms. Another study [8] highlights the role of feature selection in ML-based DDoS detection, showing that optimizing features can improve real-time detection of large-scale attacks in the 5G core network.

Our approach involves simulating various types of potential attacks originating from IIoT networks targeting the 5G core, with the goal of creating a comprehensive dataset. We utilized this dataset to train a ML model capable of detecting anomalies and intrusions within the core network. To facilitate these simulations, we have developed a robust and scalable testbed that accurately replicates the 5G core network environment. This testbed not only serves our

IoT 2024, Oulu, Finland

ACM ISBN 979-8-4007-1285-2/24/11
https://doi.org/10.1145/3703790.3703815

current research needs but is also designed to be a valuable resource for future researchers who wish to generate datasets for studying other types of network attacks. The dataset we have created is particularly useful for developing advanced machine learning models capable of detecting complex anomalies and intrusions. By providing a reliable foundation for training these models, our work contributes to enhancing the security and resilience of 5G networks against emerging threats.

Our contributions introduce several key novelties:

- **Comprehensive Attack Simulation Testbed:** We developed a cloud-native robust and scalable testbed using open-source tools to accurately simulate a wide range of IIoT-driven attacks on the 5G core network, providing a valuable resource for future research.
- **Unique Dataset Generation:** The attack simulations produced a comprehensive dataset that is specifically tailored for training machine learning models to detect complex network anomalies and intrusions in IIoT domain.
- **LSTM Autoencoder for Anomaly Detection Model:** We developed an LSTM Autoencoder model that captures both temporal dependencies and feature relationships, enabling detection of various attacks. It offers real-time monitoring for continuous and proactive anomaly detection in the 5G core.
- **Adaptability to Evolving Threats:** Our model's unsupervised learning capability enables it to adapt to new and evolving threats, including unseen attacks, without needing labeled data, ensuring sustained effectiveness over time.

This demo simulates various attack types described in Section 3, allowing the monitoring system to assess their impact on the overall system. Following this, the anomaly and intrusion detection system identifies the specific attacks, demonstrating its effectiveness in recognizing potential security threats.

2 System Setup

In our system, 5G core is deployed source tools with IIoT devices, monitoring and detection setup for simulating various IIoT-based attacks targeting the core network ensuring accessibility for future research.

2.1 System Architecture

The proposed architecture designed to simulate and study attacks initiated from IIoT devices on 5G core networks comprises a 5G Core Network with network functions, integrated with legitimate and compromised IIoT devices. Malicious IIoT launch various attacks such as GPRS Tunelling Protol - User Plane (GTP-U) Denial of Service (DoS) attacks, attach request flooding, and Packet Forwarding Control Protocol (PFCP) attacks mentioned in the section 3. To detect and analyze these security threats, the system includes a Monitoring System; integrated for metrics collection and monitoring and Anomaly/Intrusion Detection system ; for real-time anomaly and intrusion detection. This comprehensive setup allows researchers and security professionals to assess the resilience of 5G networks against different IIoT-based attack vectors. Figure 1 illustrates the system architecture.

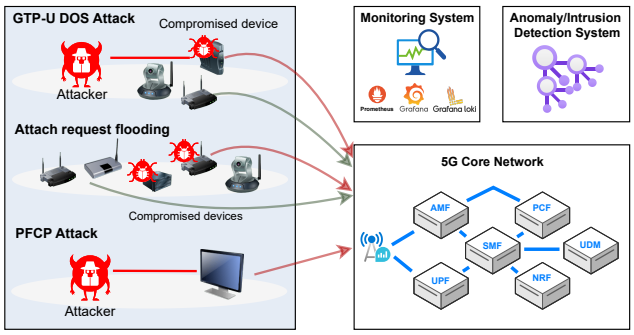

Figure 1: System Architecture.

2.2 Prototype Setup

For the simulation of attacks, the 5G core is deployed on a Kubernetes cluster, ensuring scalability and flexibility in the test bed environment. To create the test bed, we used three well-known open-source projects: Open5GS [12], UERANSIM [16], and OpenAirInterface [13]. Open5GS simulates the 5G core network elements, UERANSIM simulates legitimate IoT devices and the access network, and OpenAirInterface simulates the access network for the attacker, which is built using a USRP B210 and a Quectel modem (Figure 2).

The parameters of the core network are collected from the monitoring system, which consists of open-source applications such as Prometheus [14], Grafana [9], and Rancher [15]. These parameters are then forwarded to the anomaly and intrusion detection system for further processing.

Component	Description
Servers	Lenovo ThinkStation P3
Software Defined Radio	USRP B210
IoT Devices	Quectel modem RMU500-EV
Monitors	Lenovo ThinkStation 27"

Table 1: Prototype specifications.

3 Methodology

We generated a comprehensive dataset by simulating a range of potential attacks on the core network, alongside legitimate IIoT device operations using UERANSIM. Data was gathered during both attack scenarios and normal operational states through our monitoring system. This dataset was subsequently utilized to train the ML model, enhancing its capability to accurately detect anomalies and intrusions.

3.1 Attack Simulation

3.1.1 ***DoS Attack on the GTP-U Interface.*** The GTP-U interface is a key component in the 5G core network, responsible for the transfer of user data between the Radio Access Network (RAN) and the core network. It ensures efficient data flow by encapsulating user data packets for transmission across the network.

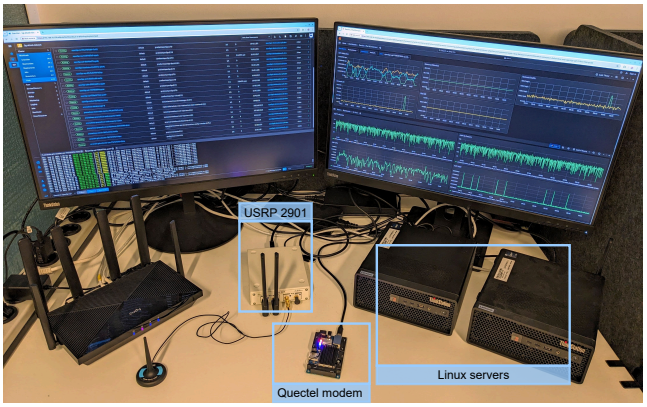

Figure 2: Testbed setup.

In our scenario, the compromised IIoT device targets the GTP-U endpoint IP located within the User Plane Function (UPF). Several types of attacks were generated using the hping3 tool, with the primary objective being to increase the resource utilization of the UPF during the attack.

3.1.2 ***Attach Request Flooding.*** In this attack scenario, we simulated a compromised IIoT device that continuously attempts to attach to the network, simulating a DDoS attack on the N1 interface of the Access and Mobility Management function (AMF). The compromised device repeatedly alters its Subscription Permanent Identifier (SUPI) to generate multiple attach requests. Although these compromised devices are unable to actually access the network, their repeated attach attempts still consume critical resources from the gNodeB, AMF, Authentication Server Function (AUSF) and Unified Data Management (UDM) systems.

3.1.3 ***DoS attack in PFCP interface.*** The Packet Forwarding Control Protocol (PFCP) interface facilitates the communication between UPF and Session Management Function (SMF), allowing for the dynamic creation, modification, and deletion of packet forwarding rules. This enables a wide range of network slicing, Quality of Service (QoS), and security policies to be implemented, supporting diverse service requirements in the 5G era.

In this attack scenario, we created a separate pod as the attacking node, which operates within the same network as the other core network nodes. Using Scapy [2], a Python framework for packet crafting, we generated fake session deletion and session modification requests. These requests were then flooded to the User Plane Function (UPF) by altering the Session Endpoint Identifier (SEID). The objective of these fake messages was to drop the sessions of legitimate users within the UPF and to exhaust its resources, thereby disrupting the normal functioning of the network.

3.1.4 ***IoT-Initiated DDoS Attack on External Servers via 5G Core Infrastructure.*** In this scenario, malicious IIoT devices exploit the 5G core network to execute a DDoS attack aimed at external servers and edge nodes. The attack is carried out by flooding the 5G network with a massive volume of malicious requests or data packets, which are then directed towards the target servers. This overwhelms the processing capacity of the servers, leading to significant service disruptions. Additionally, because the attack is routed through the 5G core network, it also consumes valuable resources within the core, potentially degrading the performance of the entire network.

3.2 Attack Demonstration

The demonstration showcases the execution of various attacks on the 5G core network, illustrating their impact through real-time monitoring using Grafana graphs (Figure 3). We will display the collected dataset that captures the network's behavior during these attacks and normal operations. Finally, we will demonstrate how our Machine Learning model, trained on this dataset, effectively detects and identifies these attacks, highlighting its potential for enhancing the security of 5G networks.

Figure 3: Monitoring Dashboard.

3.3 Data Collection

To analyze attacks on the 5G core network, we employ a comprehensive data collection approach using various monitoring tools to extract critical information. The 5G core is deployed on a Kubernetes (K8s) cluster, offering scalability and flexibility in managing network functions. Data is gathered from multiple sources, including network traffic, K8s pod metrics, logs from 5G core functions, and packet captures. This diverse data set enables thorough network behavior analysis and effective threat detection.

The primary tools include Prometheus for real-time K8s metrics (CPU, memory, disc I/O, network I/O), Loki for log aggregation from 5G core functions, and Tcpdump for capturing raw network packets, providing a low level view of the traffic passing through the 5G core, allow deep and detailed inspection of network flows. Combination of this data collectively provide insights into infrastructure performance, operational context, and deep network traffic inspection, facilitating the detection of anomalies and potential attacks.

This multi-faceted approach, integrating real-time metrics, log analysis, and deep packet inspection within a K8s-managed 5G core network, combined with a wide range of simulated IIoT-driven attacks on the 5G core provides a uniquely holistic perspective that significantly enhances the accuracy and effectiveness of detecting various sophisticated attack vectors. The simulation setup, involving 40 legitimate users across diverse threat scenarios, ensures the

dataset is both robust and representative. This research combines the simulation of IIoT-driven attacks with comprehensive monitoring tools, offering a deeper analysis and broader coverage of potential IIoT-driven security threats in 5G networks.

3.4 Detection

In this study, we use a Long Short-Term Memory (LSTM) Autoencoder Deep Learning model implemented in PyTorch to detect anomalies in a 5G core network, with a focus on identifying various DoS attacks. The LSTM Autoencoder is well-suited for this task due to its ability to capture temporal dependencies in time-series data, including network traffic metrics, Kubernetes metrics, and logs from the 5G core.

The model consists of an encoder that compresses input sequences into a fixed-length latent representation, capturing essential temporal features, and a decoder that reconstructs the original sequence. During training, the model learns from attack-free network data, minimizing the reconstruction error. When deployed for real-time monitoring, the model calculates reconstruction errors for incoming sequences; those exceeding a predefined threshold are flagged as anomalous, indicating potential DoS attacks. This threshold is determined based on reconstruction error distributions observed during training.

The LSTM Autoencoder's ability to learn and recognize temporal patterns allows it to effectively distinguish between normal operational variations and anomalies signaling malicious activity. Its unsupervised learning capability is particularly valuable for detecting new, unseen types of DoS attacks without requiring labeled data. Additionally, the model's adaptability allows for retraining with updated data, ensuring ongoing effectiveness as network behavior evolves. This makes our model a robust, scalable solution for enhancing 5G core network security through continuous, proactive anomaly detection.

4 Results

We developed a scalable and portable testbed, generated a rich dataset, and trained an ML model to detect attacks. The specifications of the current dataset are listed below (Table 2).

Description	Value
Number of Legitimate users	40
Number of hours for the data collection	48
Parameters count from POD metrics	30
Parameters count from loki logs	8
Parameters count from interface traces	15

Table 2: Specifications of the dataset

5 Conclusion and Future Work

In this study, we simulated several types of attacks originating from IIoT devices targeting the 5G core network. This simulation allowed us to create a robust dataset by collecting extensive logs, traces, and metrics from our testbed. The dataset serves as a solid foundation for analyzing various attack scenarios and evaluating system responses. We also enhanced our machine learning model to effectively detect anomalies and vulnerabilities in real-time, thereby improving its ability to identify and address security issues promptly.

Future work will focus on expanding the scope of our attack simulations to include and evaluate a broader range of IIoT-driven threats, thereby improving the comprehensiveness and robustness of our security analysis. Additionally, we aim to expand the data collection process to incorporate additional sources, such as Kubernetes syslogs which can be used to perform software integrity checks, enhancing the reach of our dataset. We also plan to refine our LSTM Autoencoder model by integrating it with other advanced machine learning techniques, such as Graph Neural Networks (GNN) and federated learning, to improve detection accuracy and scalability.

Acknowledgments

This work has been conducted as part of the Business Finland-funded 6G Cure project and supported by the 6G Flagship program under Grant 346208.

References

[1] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. 2017. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*. 1093–1110.

[2] Philippe Biondi and the Scapy community. 2024. *Scapy Documentation.* https://scapy.readthedocs.io/en/latest/ https://scapy.readthedocs.io/en/latest/.

[3] Defense Use Case. 2016. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)* 388, 1-29 (2016), 3.

[4] Sean Collins and Stephen McCombie. 2012. Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism* 7, 1 (2012), 80–91.

[5] Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. 2018. TRITON: The first ICS cyber attack on safety instrument systems. *Proc. Black Hat USA* 2018 (2018), 1–26.

[6] International Telecommunication Union (ITU). 2024. 5G: Fifth Generation of Mobile Technologies. https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx. Accessed: 2024-08-09.

[7] Hwankuk Kim. 2020. 5G core network security issues and attack classification from network protocol perspective. *J. Internet Serv. Inf. Secur.* 10, 2 (2020), 1–15.

[8] Ye-Eun Kim, Yea-Sul Kim, and Hwankuk Kim. 2022. Effective Feature Selection Methods to Detect IoT DDoS Attack in 5G Core Network. *Sensors* 22, 10 (2022). doi:10.3390/s22103819

[9] Grafana Labs. 2024. Grafana: Documentation. https://grafana.com/docs/grafana/latest/. Accessed: 2024-08-08.

[10] Jiaqi Li, Zhifeng Zhao, and Rongpeng Li. 2018. Machine learning-based IDS for software-defined 5G network. *IET Networks* 7, 2 (2018), 53–60. doi:10.1049/iet-net.2017.0212 arXiv:https://ietresearch.onlinelibrary.wiley.com/doi/pdf/10.1049/iet-net.2017.0212

[11] Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum, and Nasir Ghani. 2019. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Communications Surveys & Tutorials* 21, 3 (2019), 2702–2733. doi:10.1109/COMST.2019.2910750

[12] Open5GS. 2024. Open5GS. https://open5gs.org/. Accessed: 2024-08-01.

[13] OpenAirInterface. 2024. OpenAirInterface - Open-source 5G Platform. https://github.com/OPENAIRINTERFACE/openairinterface5g Accessed: 2024-08-08.

[14] Prometheus. 2024. Prometheus: Overview. https://prometheus.io/docs/introduction/overview/. Accessed: 2024-08-08.

[15] Rancher Labs. 2023. Rancher: Open-Source Kubernetes Management. https://rancher.com/. Accessed: 2024-08-26.

[16] UERANSIM. 2024. UERANSIM. https://github.com/aligungr/UERANSIM. Accessed: 2024-08-01.

[17] Dan Wang, Dong Chen, Bin Song, Nadra Guizani, Xiaoyan Yu, and Xiaojiang Du. 2018. From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies. *IEEE Communications Magazine* 56, 10 (2018), 114–120. doi:10.1109/MCOM.2018.1701310

[18] Meisu Zhong, Yongsheng Yang, Haiqing Yao, Xiuwen Fu, Octavia A. Dobre, and Octavian Postolache. 2019. 5G and IoT: Towards a new era of communications and measurements. *IEEE Instrumentation & Measurement Magazine* 22, 6 (2019), 18–26. doi:10.1109/MIM.2019.8917899