electronics

MDPI

Article

Cyber5Gym: An Integrated Framework for 5G Cybersecurity Training

Muhammad Ali Hamza [†], **Usama Ejaz** [†] and **Hyun-chul Kim** [*]

Department of Software, Sangmyung University, Cheonan 31066, Republic of Korea; alihamzaiub13@gmail.com (M.A.H.); usamaijaz404@gmail.com (U.E.)

[*] Correspondence: hyunchulk@gmail.com

[†] These authors contributed equally to this work.

Abstract: The rapid evolution of 5G technology, while offering substantial benefits, concurrently presents complex cybersecurity challenges. Current cybersecurity systems often fall short in addressing challenges such as the lack of realism of the 5G network, the limited scope of attack scenarios, the absence of countermeasures, the lack of reproducible, and open-sourced cybersecurity training environments. Addressing these challenges necessitates innovative cybersecurity training systems, referred to as “cyber ranges”. In response to filling these gaps, we propose the Cyber5Gym, an integrated cyber range that enhances the automation of virtualized cybersecurity training in 5G networks with cloud-based deployment. Our framework leverages open-source tools (i) Open5GS and UERANSIM for realistic emulation of 5G networks, (ii) Docker for efficient virtualization of the training infrastructure, (iii) 5Greply for emulating attack scenarios, and (iv) Shell scripts for automating complex training operations. This integration facilitates a dynamic learning environment where cybersecurity professionals can engage in real-time attack and countermeasure exercises, thus significantly improving their readiness against 5G-specific cyber threats. We evaluated it by deploying our framework on Naver Cloud with 20 trainees, each accessing an emulated 5G network and managing 100 user equipments (UEs), emulating three distinct attack scenarios (SMC-Reply, DoS, and DDoS attacks), and exercising countermeasures, to demonstrate the cybersecurity training. We assessed the effectiveness of our framework through specific metrics such as successfully establishing the 5G network for all trainees, accurate execution of attack scenarios, and their countermeasure implementation via centralized control of the master using automated shell scripts. The open-source foundation of our framework ensures replicability and adaptability, addressing a critical gap in current cybersecurity training methodologies and contributing significantly to the resilience and security of 5G infrastructures.

Keywords: 5G; cybersecurity; cyber range; Open5GS; UERANSIM; threats; vulnerabilities; training system

check for updates

Citation: Hamza, M.A.; Ejaz, U.; Kim, H.-c. Cyber5Gym: An Integrated Framework for 5G Cybersecurity Training. *Electronics* **2024**, *13*, 888. https://doi.org/10.3390/electronics13050888

Academic Editors: Cheng-Chi Lee and Tuan-Vinh Le

Received: 30 January 2024
Revised: 19 February 2024
Accepted: 21 February 2024
Published: 26 February 2024

1. Introduction

The evolution of 5G technology has brought significant improvements in speed, capacity, reliability, and connectivity, fundamentally transforming the telecommunications landscape [1]. Yet, these rapid advancements bring significant cybersecurity challenges [2,3] such as introducing new vulnerabilities [4,5], highlighting the need for robust cybersecurity measures [6,7]. The inherent complexity [8] and critical nature of these networks [9] further necessitate advanced cybersecurity measures. The hands-on training of defenders is essential to equipping them with the skills to identify and mitigate emerging threats. For instance, cybersecurity systems such as 5Greplay [10], 5Greasoner [11], and the training environment exemplified by SPIDER [12] play a vital role in this process, offering experiences that foster proficiency in managing and defending against cyberattacks. These platforms provide invaluable insights into potential 5G network vulnerabilities and hands-on experience in navigating real-world cyberattack scenarios. This foundational knowledge is crucial for ensuring the security and integrity of 5G infrastructure, which supports a wide range of applications, from industrial automation to critical communication services [1]. cybersecurity training system for 5G networks, offering hands-on experience with real-time attack and defense scenarios through the use of open-source tools. Our framework can be viewed as an integrated cybersecurity training system for 5G networks, offering hands-on learning experience with real-time cyberattack and defense scenarios through the use of open-source tools.

Despite advancements in 5G network technologies, the current cybersecurity tools and training systems encounter significant challenges. For instance, 5Greplay [10] focuses on emulating attack scenarios and lacks comprehensive defensive strategies and a cybersecurity training environment. Moreover, the 5Greasoner [11] primarily focuses on implementing Finite State Machine (FSM) code rather than deploying a simulated 5G network environment for security attack implementation. This approach may limit the practical applicability of 5Greasoner in real-world 5G network scenarios, where direct implementation and testing of security strategies are crucial. Studies such as [3,13] demonstrate the importance of cyber ranges for automated and virtualized cybersecurity training and experimentation. Similarly, the SPIDER [12,14] cyber range, though providing a comprehensive approach to manage and emulate complex network environments, cannot be replicated due to the closed-source nature of their 5G network environments. Its reliance on attack scenarios based on synthetic traffic generation limits the scope of simulated cyber threats. This gap is evident in the lack of automated training systems that can be replicated and effectively prepare cybersecurity experts for the multi-layer threats and vulnerabilities inherent in 5G infrastructure.

To address these emerging challenges in training cybersecurity experts for 5G networks, we introduce an integrated, comprehensive solution that offers a dynamic learning environment tailored to the complexities of 5G network security. Our framework emphasizes an integrated training approach for the emulation of 5G networks, real-time attack scenarios, and defensive strategies. This benchmark system is poised to significantly enhance the capabilities of cybersecurity professionals, equipping them with the skills necessary to protect the intricate and critical infrastructure of 5G networks, and has the potential to adapt to the evolving threat landscape. We highlight the main contributions of this paper as follows:

(a) We present Cyber5Gym, an integrated cybersecurity training system that offers an emulation of the 5G network infrastructure, including the implementation of 5G services: User Equipment (UE), Radio Access Network (RAN), and Core Network (CN). It fills the gap by (i) offering a hands-on training experience for emulating 5G network environments using open sourced tools such as Open5GS [15] and UERANSIM [16], along with real-time attack scenarios incorporating defensive strategies, and (ii) enhancing its operational efficiency through the automation and virtualization of its training modules, utilizing Docker for virtualization and Shell scripts for automation of tasks. Additionally, we have deployed our system on Naver Cloud for demonstration. The integration of open-source tools for 5G network emulation, along with the implementation of multiple attack scenarios and their countermeasures, makes our cyber range replicable, extendable, and scalable.

(b) Our proposed system offers a cybersecurity training environment that is adaptable for both individual learning and the development of multi-users. The system is designed for a dynamic number of participants, though centralized control is achieved through a master server, which enriches the training process within a managed environment. This system is crucial for conducting synchronized attacks from multiple points and for crafting coordinated countermeasures. This kind of training ground is imperative for equipping cybersecurity experts with the skills necessary to address evolving challenges in 5G network security, thereby playing a significant role in bolstering the robustness and defense of essential 5G infrastructures.

(c) The Cyber5Gym testbed is designed to offer the hosts (trainees) a series of realistic 5G network emulations, such as autonomous operational tasks to configure all host networks and execute intricate cyberattack scenarios and their countermeasures. Trainees are exposed to advanced threats as use cases, such as NAS-5G SMC Replay attacks, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks. This diversity in attack scenarios equips trainees with a hands-on understanding of cybersecurity threats and their countermeasures. Furthermore, the automation scripts are used to perform autonomous operational tasks such as 5G network emulation and monitoring the log activities of trainees. These scripts are pivotal in enabling the master server to securely connect with individual trainee hosts, thereby facilitating seamless 5G networking across all trainee setups.

(d) We showcased a comprehensive evaluation by deploying our framework at Naver Cloud, involving 20 trainees, each of them accessing an emulated 5G network and managing 100 UEs. Our assessment focused on key metrics, including the successful establishment of the 5G network, accurate execution of attack scenarios, and the efficient deployment of countermeasures through automated shell scripts. This evaluation not only validates the effectiveness of the deployment of our framework in real-world conditions but also highlights its potential to significantly enhance the resilience and security of 5G infrastructures through the open-source, replicable, and adaptable foundation of our training system.

The structure of the paper is organized as follows: Section 2 delves into the background. Section 3 presents an overview of the existing literature relevant to 5G cybersecurity training systems. Section 4 details the proposed system architecture. In Section 5, we demonstrate the implementation of the proposed system with 5G emulation, attack scenarios, and countermeasures. In Section 6, we assess the Cyber5Gym framework, focusing on its limitations, scalability, security, and prospective enhancements in 5G cybersecurity training. Finally, Section 7 concludes the paper and outlines future directions.

2. Background

2.1. Cyber Ranges

Cyber ranges, initially developed for military use, have expanded into industrial, academic, and commercial areas [17]. These environments blend physical and virtual elements to simulate real-world cyber scenarios, enhancing practical learning through active engagement. They now support specialized domains such as Internet of Things (IoT) [18], cyber-physical systems [19], smart grids [20], and Information Communications Technology (ICT) systems [12,14,21]. Furthermore, the cyber ranges serve various purposes: research and development, training and education [3,22], and hosting exercises and competitions like Cyber Defense Exercises (CDX) and Capture the Flag (CTF) events [23]. Some other researchers have created flexible, scalable, and easily reproducible cybersecurity environments for training and experimentation by leveraging AI [13], virtualization [3,24], and automation tools, using technologies like Docker, Ansible, and Python. These works on cyber range inspire us to propose Cyber5Gym, an integrated cyber range that enhances cybersecurity training by automating the emulation of diverse 5G network environments. Our Cyber5Gym features different roles, such as master and trainees, and includes various attack scenarios with their countermeasures, providing a comprehensive and dynamic learning experience for modern 5G security challenges.

2.2. 5G Architecture

The architecture of the 5G system can be broadly categorized into three primary components [11]: the User Equipment (UE), the Radio Access Network (RAN), and the Core Network (CN) (see Figure 1). Each of these components plays a pivotal role in the functionality and efficiency of the 5G network, ensuring high-speed connectivity and advanced network capabilities.

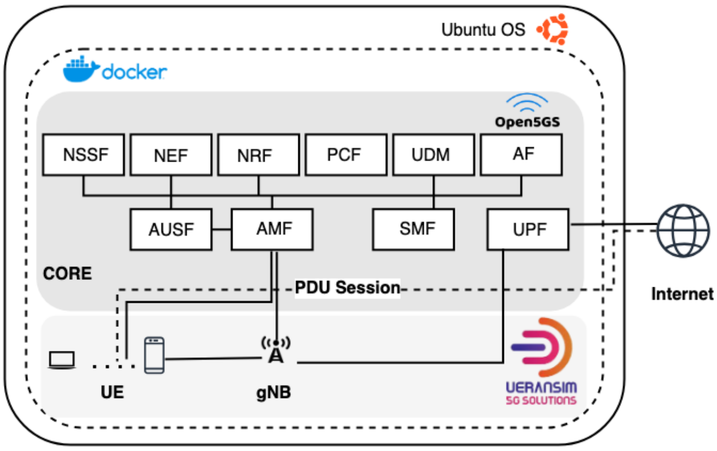


Figure 1. Simplified Virtualized 5G Architecture.

User Equipment (UE): The UE refers to the devices that end-users utilize to connect to the 5G network. These include a wide array of devices, from smartphones and tablets to a multitude of IoT devices. UEs are not just communication endpoints but are integral to managing sophisticated tasks like processing power and storage, thereby facilitating a more distributed network architecture. Moreover, UE is crucial for testing and emulating the behavior of real-world devices within the 5G network. It allows for the evaluation of network performance and the effectiveness of various network configurations and security protocols from the perspective of the end user.

Radio Access Network (RAN): The RAN is the link between the UE and the Core Network. It consists of base stations and other radio access nodes that facilitate wireless communication with mobile devices. In 5G networks, the RAN is developed to support a higher frequency spectrum and advanced technologies such as Massive MIMO (Multiple Input Multiple Output) and beamforming. These technologies are key to achieving the high data rates, reduced latency, and enhanced capacity that 5G promises.

Core Network (CN): The Core Network is the backbone of the 5G system, orchestrating the management and delivery of services. It is responsible for critical functions such as data routing, authentication, session management, and mobility management. The CN is more software-centric in 5G, offering flexibility and scalability to accommodate the diverse needs of different applications, ranging from high-speed internet access to critical communication for autonomous vehicles and industrial automation. Within the CN, three essential elements play key roles:

1. Access and Mobility Management Function (AMF): The AMF is fundamental in managing user connectivity and ensuring seamless mobility. It is responsible for authentication, security control, and session management. The AMF ensures that as devices move, maintain continuous and secure connectivity, switching between different access networks when needed.
2. Session Management Function (SMF): This function primarily deals with session establishment, modification, and release. It manages the data sessions for each user, ensuring that the network resources are allocated effectively and that the data routing paths are optimized for each session. The SMF plays a crucial role in quality of service (QoS) management and in enforcing data policies.
3. User Plane Function (UPF): The UPF is involved in data plane processing, including packet routing and forwarding. It serves as the anchor point for intra-network and inter-network mobility, enabling user data to be transferred seamlessly across the

network. The UPF is crucial for achieving the high data rate and low latency features that are characteristic of 5G networks.

2.3. 5G Interfaces

The standard 5G network architecture includes key interfaces such as N1, N2, N3, and N4, each critical for network functionality and management [25].

N1 Interface: The N1 interface connects the UE to the network, specifically linking the UE with the AMF. This interface is crucial for the initial registration of the UE to the network, authentication, session management, and mobility management. It carries signaling messages that facilitate these functions and ensure that the UE can effectively communicate with the core network for necessary services. From a cybersecurity perspective, it is a crucial point of vulnerability before the establishment of a security context, as NAS messages are unencrypted and susceptible to interception. As demonstrated in our training scenarios, a malicious actor with access to the N1 interface could manipulate NAS messages, underscoring the necessity of stringent security measures in the early communication stages. For example, SMC-reply attack, where attackers can intercept and replay security mode commands.

N2 Interface: The N2 interface is established between the AMF and the Next Generation NodeB (gNB), which is part of the RAN. This interface plays a key role in controlling the flow of data and managing the resources of the radio network. It is responsible for setting up bearers, managing mobility, and handling the control plane information that dictates how data is routed and managed within the RAN. Moreover, the importance of the N2 interface in cybersecurity training environments such as Cyber5Gym, lies in demonstrating how an attacker might disrupt bearer setups or manipulate control plane information, thereby undermining network stability.

N3 Interface: The N3 interface is the data pathway between the gNB in the RAN and the UPF in the Core Network. This interface is crucial for the actual transmission of user data. It handles the data packets coming from the user equipment, passing them through the RAN and forwarding them to the Core Network for routing to their final destination. The N3 interface is integral to achieving the high-speed data transmission capabilities of 5G, facilitating the core data transport function of the network. While N3 facilitates high-speed data, it also poses a risk of data interception and requires comprehensive security protocols, a focus in our DDoS simulations where trainees learn to secure data transmission pathways.

N4 Interface: The N4 interface connects the SMF with the UPF. This interface is used for the management and control of user plane sessions. It allows the SMF to establish, modify, and release session contexts in the UPF. Through the N4 interface, the SMF can control and manage the flow of data, ensuring that routing paths are optimized and that the quality of service requirements for each user session are met. It makes the N4 interface a potential target for attacks aimed at disrupting session contexts, which our training scenarios address by teaching trainees to maintain session integrity and respond to threats dynamically. In cybersecurity training systems, trainees need to learn to secure this interface, reinforcing its role in safeguarding user plane sessions against unauthorized modifications.

Collectively, these components and interfaces form the backbone of the 5G network, enabling it to support a wide range of applications and services with unprecedented speed and reliability [11].

2.4. 5G Security Threats

The transition to 5G networks has introduced a wide range of security challenges that extend beyond traditional network threats. Advances in technology that enable higher data rates and connectivity also expose networks to new attack vectors and vulnerabilities [4,5,26]. The complexity of 5G networks, from their distributed architecture to the use of ML for network management, introduces security risks that can manifest in various forms [4,11,26,27].

In this complex security landscape of 5G networks, the Radio Resource Control (RRC) and Non-Access Stratum (NAS) Security Mode Command (SMC) messages play critical roles in the security and connection setup between UE and the network. However, these messages can become a vector for attacks if not properly secured [5]. These messages, crucial for secure communication, can be exploited through sophisticated cyber threats like the NAS-5G SMC Replay Attack [10]. This attack exploits the replay of an NAS SMC message, potentially granting unauthorized access and leading to data interception. The NAS-5G SMC emerges as a sophisticated cyberattack within the 5G telecommunication domain. This malicious activity entails the replication and subsequent retransmission of an NAS SMC message previously intercepted [10]. The execution of such an attack leads to the deception of network security protocols, resulting in the misidentification of an unauthorized device as a legitimate entity within the network. This breach in security protocol opens avenues for unauthorized access, significantly heightening the risk of sensitive data interception and compromise. The implications of such a vulnerability are extensive, undermining the fundamental tenets of integrity and confidentiality in communications across the 5G infrastructure. This situation thus underscores the urgency for the development and implementation of robust security measures equipped to detect and thwart such sophisticated cyberattacks.

Apart from the NAS-5G SMC Replay Attack, 5G networks face threats like Advanced Persistent Threats (APTs), which use stealthy and continuous hacking processes to gain prolonged access to networks, and Man-in-the-Middle (MitM) attacks [28], exploiting the dynamic network slicing capabilities of 5G. Additionally, the seamless connectivity feature of 5G is vulnerable to Distributed Denial of Service (DDoS) attacks because malicious actors can exploit the enhanced connection and bandwidth attributes of the network infrastructure [4]. In such attacks, compromised devices, often part of a botnet, inundate the network with excessive traffic. This can lead to server overloads, service disruptions, and, in severe cases, complete network shutdowns. The distributed nature of 5G networks amplifies their vulnerability to these attacks, demanding adaptive and robust security measures for detection and mitigation. Furthermore, Denial of Service (DoS) attacks in 5G specifically target the high throughput capabilities of the network, differing from traditional DDoS attacks that primarily aim to overwhelm network capacity [10]. These high-bandwidth attacks lead to significant network congestion, degraded service quality, and in extreme scenarios, total network failure. The challenges posed by such attacks, given the high data capacity, underscores the need for advanced detection and mitigation strategies to maintain network stability and reliability.

Persistent Packet Data Unit (PDU) session attacks in the 5G core network, such as the Persistent Session Deletion and Persistent Session Modification attacks, involve a malicious entity exploiting the Packet Forwarding and Control Protocol (PFCP) to compromise end-user connectivity to the Data Network (DN) [26]. These attacks target the communication between the Session Management Function (SMF) and User Plane Function (UPF) on the N4 interface. By manipulating PFCP messages, attackers can disconnect a UE from the DN or modify its session to drop all packet handling rules, maintaining the UE's connection to the 5G RAN and core network. These session-targeting attacks are extended to IP-targeting ones by correlating the target UE's IP address with its Session Endpoint Identifier (SEID) during handovers. This approach introduces a persistent layer to these attacks, allowing loss of connectivity to follow the UE despite changes in SEIDs, IP addresses, or Tunnel Endpoint Identifiers (TEIDs). This newly introduced persistence layer requires more intricate attack strategies and highlights the need for robust mitigation measures within the 5G core.

These varied attacks highlight the critical need for specialized cybersecurity training platforms. Implementing cyber ranges that offer realistic, emulation-based environments is essential for developing the next generation of cybersecurity experts who are adept at navigating and mitigating the complex security challenges of 5G networks.

3. Related Work

In recent years, significant advancements have been made in the development of 5G networks, with particular emphasis on enhancing their security and robustness. The work of [27] developed a 5G testbed designed for evaluating performance and security vulnerabilities in network slices. Utilizing OpenAirInterface [29], this testbed integrates both CN and RAN components, employing the OAI Simulator [30] for the emulation of UE and RAN. Within this framework, network slices are represented by Docker Containers instead of separate network functions. Furthermore, other studies such as [11,31–33] conduct a comprehensive analysis of platforms and frameworks for implementing Core Network. Comparing Magma [33], Open5GS [15], and Free5GC [34], their study aims to evaluate development and computational efficiency, emphasizing flexibility, scalability, and resource utilization. Their findings motivate us to utilize Open5GS for the implementation of the CN components in our 5G system.

Further advancements in 5G security research are evident in studies focusing on specific threat vectors and vulnerabilities. The work in [26] is crucial in providing comprehensive datasets that encompass both IP-layer and Core Network attacks, facilitating the development of more effective security solutions. Concurrently, research works [7,25] have highlighted critical vulnerabilities such as the susceptibility of 5G networks to DoS attacks and security header type attacks. Previously, refs. [28,35–37] explored the automation test coverage to spot issues and potential security vulnerabilities in 4G and Long Term Evolution (LTE) networks. For instance, ref. [38] investigates the security aspects of control plane procedures based on dynamic testing of the control components in operational LTE networks. Aside from this, ref. [39] has explored the integration of AI with 5G technologies, and [13] explores technological advancements in intelligent cyber ranges, focusing on AI applications for improving cybersecurity training and experimentation. These studies highlight the integration of AI in creating dynamic and realistic cyber attack scenarios, enhancing the effectiveness of cybersecurity training. Similarly, the work of [27] has contributed to understanding dynamic network slicing, essential for accommodating diverse service demands. These studies lay the foundation for understanding the complex interplay between advanced network functionalities and security considerations in 5G network environments.

The exploration of practical tools for testing and enhancing 5G network security has also been a focal point in recent research. The introduction of 5Greplay [10] marks a significant step forward, providing a means to assess the resilience of 5G network components against diverse attack scenarios. It is an open-source 5G network traffic fuzzer designed to evaluate 5G components by replaying, modifying 5G network traffic, and injecting network scenarios into a target, which can be a 5G service such as Core Network (e.g., AMF, SMF) or a RAN network (e.g., gNodeB). This aligns with study [40] that explores the inherent weaknesses of 5G technology and underscores the pressing need for robust defense mechanisms. Such research is pivotal in developing comprehensive strategies to counteract emerging security threats in 5G networks. The work of [12,14] demonstrates the use of a cyber range platform, SPIDER, for training cybersecurity professionals. Integrating machine learning-driven security analytics, this platform facilitates network traffic emulation and attacker connection detection. However, the implementation details of the 5G network environment are less transparent, probably due to its closed-source nature, which might limit the ability to reproduce or extend this training method in real-world cybersecurity scenarios. Incorporating these insights, it can be concluded that such reproducible training environments are crucial for enhancing the skills of defenders in identifying and mitigating cyberattacks in 5G networks.

The existing works in 5G cybersecurity training are instrumental but have limitations such as lack of realism [11], limited scope of attack scenarios [10,26,35], absence of comprehensive countermeasures [10,25,40], and the challenge of reproducibility [12,14]. This paper distinguishes itself from the abovementioned studies by presenting a comprehensive approach to training and evaluating cybersecurity defenders in a realistic 5G network environment. While previous research [10,12,25,26,35,40] has primarily focused on individual aspects of 5G security, such as network slicing, specific threat vectors, or the development of testing tools, our work integrates these insights to address the unique security challenges and vulnerabilities inherent in 5G networks. We propose an autonomous cybersecurity system, contextualized within the broader narrative of 5G security challenges, that is capable of emulating real-world 5G attack scenarios. This system not only demonstrates effective defense mechanisms against these sophisticated threats but also fills the gaps left by existing research, thereby significantly contributing to the resilience of 5G networks against emerging cyberattacks.

4. Cyber5Gym Architecture

The Cyber5Gym system presents a comprehensive architecture designed to facilitate cybersecurity training in 5G networks. The architecture of our framework is founded on a Docker-based virtualization framework, designed to create a lightweight yet efficient emulation environment for both 5G network components and cybersecurity scenarios. At its core, the system employs Open5GS for simulating core network functionalities and UERANSIM for the radio access network (RAN) emulation, thereby facilitating a detailed and comprehensive representation of 5G network operations. Docker containers ensure an easily replicable setup and flexible adaptation to a wide range of training requirements. To enhance the realism of cybersecurity training, the 5Greply tool has been incorporated for the accurate emulation of attack scenarios, including but not limited to SMC-Reply and DoS attacks. This inclusion further enriches the training environment with practical, hands-on experience in identifying, responding to, and mitigating potential security threats within a 5G context. Further details of these key components include:

1. **Virtualization with Docker**: Docker, an open-source container platform, excels in orchestrating a lightweight virtual environment conducive to code execution, application migration, and enhanced project collaboration. Docker notably surpasses Virtual Machines (VMs) in execution and startup efficiency, demonstrating at least a fifty percent enhancement in performance [41,42]. The containerization technique inherent in Docker not only streamlines scalable, on-demand service delivery but also significantly curtails IT operational expenses. In contrast, VMs, conceptualized as software constructs within a host environment, offer extensive operating system functionalities appropriate for a broad spectrum of software applications, yet their efficiency is comparatively subdued when placed against Docker containerized approach. Thus, Docker is employed to create a virtualized environment, hosting different network elements, attack emulations, and countermeasures, offering a realistic and adaptable training environment.
2. **Open5GS and UERANSIM**: Open5GS [15], an open-source software, implements the core functionalities of the Core Network and Evolved Packet Core (EPC), enabling the creation of private and commercial network solutions. UERANSIM [16], a 5G RAN emulation tool, simulates 5G base stations (gNodeB) and UE for network protocol testing and scenario emulation. These components are crucial for providing a genuine 5G network emulation environment, essential for hands-on cybersecurity training.
3. **5Greplay [10]**: The 5Greplay [10], is an open-source 5G network traffic fuzzer designed to evaluate 5G components by replaying and modifying 5G network traffic and injecting network scenarios into a target, which can be a 5G core service (e.g., AMF, SMF) or a RAN network (e.g., gNodeB). We have utilized 5Greplay for recreating attack scenarios, enhancing the training experience with realistic cyberattack emulations.
4. **Shell Scripts**: The Shell scripts are designed to ensure efficient task coordination and execution across the master and trainee systems, streamlining the operational workflow as shown in the Algorithms 1 and 2. These scripts are also critical in managing the Docker containers, ensuring efficient deployment, configuration, and interaction of network elements. Script Automation streamlines network operations by elimi-

nating the need for manual instantiation of components such as instances, volumes, security groups, floating IPs, and images. This efficiency is manifested through a YAML-formatted text file, which enables the automation of dynamic resource management using shell scripts. A salient feature of this framework is its capacity for one-click execution via a single script, simplifying the deployment and administration of intricate network configurations. This includes the facilitation of a 5G network emulation across all hosts. Furthermore, the framework adeptly manages attack scenarios and countermeasures, leveraging distinct, purpose-specific scripts for each unique challenge, all executable with a single click.

The implementation of Cyber5Gym is designed to offer a dynamic and comprehensive training environment by integrating open-source tools, as illustrated in Figure 2. It leverages Docker for the creation of virtualized network environments for multi-users, crucial for emulating realistic 5G network scenarios. The shell scripts enhance the automation of operations, facilitating the deployment and interaction of network components. The 5Greplay tool plays a pivotal role in emulating attack scenarios. The integration of Open5GS and UERANSIM components ensures an authentic and holistic 5G network training experience, preparing cybersecurity professionals for the complexities of real-world 5G network security challenges. In the Cyber5Gym system, the primary actors are the master and the trainees:

1. **Master**: In the Cyber5Gym system, the master server plays a critical role in both establishing 5G networks and in the emulation of specific cybersecurity threats, including SMC Replay attacks, DoS, and DDoS attacks and countermeasures. Leveraging automation scripts, it coordinates emulations, training scenarios for trainee modules, and monitoring real-time trainees logs. This server also consistently updates these scenarios to reflect the latest in cybersecurity threats and defenses, maintaining the relevancy and effectiveness of the training. For a detailed overview of these emulation automation scripts, Algorithm 1 offers a high-level description.
2. **Trainees**: Within the Cyber5Gym system, trainees are key participants who undertake hands-on training, engaging with individualized 5G network emulations. These emulations provide a virtualized environment including UEs, RAN, and essential CN components, enabling trainees to immerse themselves in a range of cybersecurity challenges. Algorithm 2 provides an overview of these emulation scripts. By actively interacting with these simulated network infrastructures, trainees develop practical skills to identify and counteract potential security threats in a controlled yet realistic 5G context, enhancing their readiness for real-world cybersecurity scenarios.

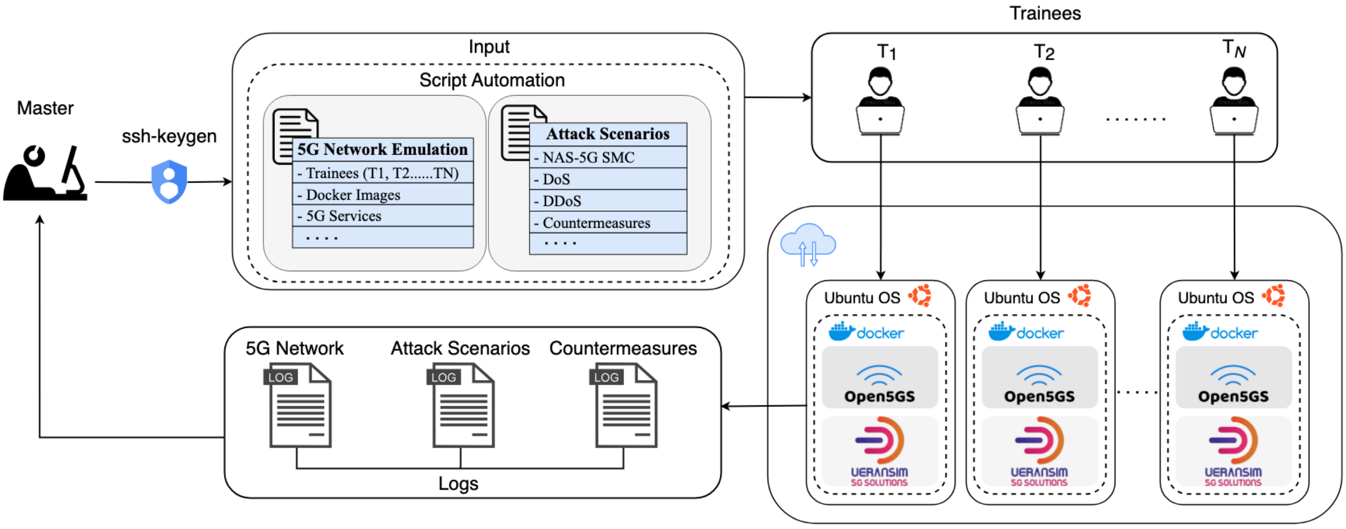


Figure 2. Architecture of the Cyber5Gym virtualized testbed, representing Trainees as T_1, T_2, ... T_N.

Algorithm 1: 5G Network Management Script using Master Server

```
Input: num_ue_containers, gNB_services, UE_Services, host_nodes, port_number
Output: Establish 5G Network in All Hosts
Procedure Manage5GNetworkServices:
    for username, host_node in host_nodes do
        ExecuteSSHCommands(username, host_node, port_number);
    end
Function ExecuteSSHCommands(username, host_node, port_number):
    RestartContainer("5G_RAN", host_node);
    for i in range 1 to num_ue_containers do
        container_name ← "5G_UE" + i;
        RestartContainer(container_name, host_node);
        ExecuteService(container_name, gNB_Services);
        ExecuteService(container_name, UE_Services);
    end
    Wait for all services to start;
    for i in range 1 to num_ue_containers do
        container_name ← "5G_UE" + i;
        CheckIPStatus(container_name, host_node);
    end
Function RestartContainer(container, host_node):
    Execute "docker restart " "container" on "host_node";
    Log restart status;
Function ExecuteService(container, command):
    Execute command in container;
    Log execution status;
Function CheckIPStatus(container, host_node):
    Check IP configuration status in container;
    Log IP status;
```

Algorithm 2: Trainee Host Setup Script for 5G Network Establishment

```
Input: docker_image_and_compose_directory, num_ue_containers
Output: Configure Trainee Host and Establish 5G Network
Procedure DeployAndConfigure5GSystem:
    UpdateSystem();
    InstallDockerComponents();
    for i ← 1 to num_ue_containers do
        imageName ← "ueimage" + i + ".tar";
        LoadDockerImage(image_and_compose_directory, imageName);
    end
    DockerComposeUp(image_and_compose_directory);
    ExecuteInContainer("5G_UE_Attacker", "Install 5GReplay Fuzzer");
    ExecuteInContainer("5G_UE_Attacker", "ConFigure 5GReplay Fuzzer");
    for i ← 1 to num_ue_containers do
        ModifyIMSINumbers("UE" + i);
    end
return
```

The Cyber5Gym framework is designed to cater to a diverse clientele, encompassing cybersecurity professionals, network engineers, and students specializing in network security. The system's adaptability allows it to serve not only as a training platform for individual learners but also as a collaborative environment for team-based cybersecurity exercises. This inclusive approach ensures that a broad spectrum of users, from beginners to advanced practitioners, can benefit from the realistic emulation of 5G network scenarios and cybersecurity threats.

The Cyber5Gym provides such environment where actors work collaboratively to create a realistic training environment, emulating 5G network and cybersecurity incidents to provide a comprehensive learning experience for the trainees, including a number of benefits as follows:

1. **Scalability:** The Cyber5Gym, with its flexible container orchestration platform, dynamically adjusts to varying demands. This allows cyber range environments to seamlessly adapt to changes in the number of trainees, the number of UE devices, or workloads, with minimal manual intervention. Additionally, we have tested its scalability, successfully accommodating up to 100 users in simulations conducted within individual Docker containers, demonstrating the flexibility and suitability of our system for a dynamic number of trainees.
2. **Automation:** Leveraging Docker and shell scripts, the system centralizes control at the master for automating critical cyber range operations. This includes deploying and scaling trainee environments in alignment with the number of UEs, orchestrating 5G network emulations across all trainee modules, and systematically executing attack scenarios and countermeasures. This centralized automation approach streamlines the management process, ensuring a consistent and efficient execution of complex 5G network training exercises.
3. **Reproducibility:** The integration of open source tools in Cyber5Gym addresses a key challenge in virtual 5G cybersecurity research: the reproducibility of methodologies and outcomes. In the field, a common issue is the non-replicability of results due to the unavailability of detailed virtual environment setups used in experiments. Our system ensures that these details are accessible and transparent, thereby not only validating the research findings but also promoting their application within the community. This approach is essential for verifying result validity and fostering the adoption of these methods in wider research contexts.
4. **Extensibility:** Our system facilitates straightforward extensions and modifications by researchers and practitioners. It specifically allows the integration and testing of novel elements, such as attack scenarios and their countermeasures and implication monitoring. Additionally, the system is equipped to compare these new features against its current capabilities, providing a comprehensive framework for continuous enhancement and evaluation in the realm of 5G cybersecurity.
5. **Portability:** The portability of containers facilitates effortless replication or relocation of cyber range environments, ensuring adaptability to various settings as required. This includes transitioning between Docker-based local environments and cloud-based deployments. For example, we have test our system by deploying it on Naver Cloud, showing that it can be deployed on any cloud platform.
6. **Cost-effectiveness:** Containerization offers a more economical approach compared to traditional virtual machines, cutting down on hardware and software expenses while enhancing resource efficiency.
7. **Resource Efficiency:** Due to their lightweight nature, Docker Containers consume fewer resources than virtual machines. This allows for a larger number of UE devices to be deployed as containers on a single host, thus optimizing resource usage and reducing cost.

5. System Implementation and Demonstration

In this section, we delve into the implementation details of the Cyber5Gym framework's deployment, highlighting the streamlined operational procedures designed to facilitate an integrated training environment. This includes a "single-click" automation strategy that simplifies the multi-server training process into three distinct steps: establishing a secure 5G network, setting up multiple UEs, and executing real-time attack scenarios alongside their countermeasures. The subsections outline the system environment demonstration, showcasing how the master server employs script automation to orchestrate the emulation of 5G network scenarios, attack simulations, and targeted counteractions across all trainee modules. This automation not only ensures a seamless setup of Docker and 5G network components for each trainee but also centralizes control for synchronized training, thereby enhancing the realism and effectiveness of cybersecurity training within a 5G context.

Our evaluation further extended to a practical deployment on Naver Cloud, engaging 20 trainees in a hands-on demonstration of the Cyber5Gym framework's operational capabilities, as illustrated in Figure 5. Each trainee was allocated a virtualized instance of the Ubuntu operating system, managing a comprehensive simulation of a 5G network infrastructure. This 5G network utilizes Open5GS and UERANSIM to create a realistic emulation of 5G operations, which includes 100 user equipment (UEs) along with the Core and Radio Access Network (RAN). We have shown the successful execution of this exercise, from the establishment of the 5G network to the accurate deployment of attack scenarios and countermeasures through automated scripts. This endeavor was pivotal in demonstrating the efficacy of our framework in a multifaceted training environment, showcasing its relevance and utility in addressing real-world cybersecurity challenges within 5G networks.

5.1. System Overview

The master server orchestrates script automation, seamlessly executing 5G network emulations, real-time attack scenarios, and targeted countermeasures across all connected hosts via distinct single-click operations. The single-click operations streamline multi-server training into a three-step process for an integrated training environment:

1. Firstly, it ensures secure master-to-trainee connections using ssh-keygen, crucial for emulating authentic 5G scenarios, as shown in Figure 3.
2. Secondly, it automates the 5G network setup, configuring Docker and 5G network components such as UE, RAN, and CN for each trainee, as described in Algorithm 2 (demonstrated in the Appendix A). Moreover, the Figure 4 shows the emulations of the 5G network for multiple users using a single-click operation executed by the master (demonstrated in Appendix B).
3. Lastly, the master server orchestrates network emulations with multiple UEs as depicted in Figure 5, including cyberattacks and countermeasures, with centralized control to synchronize training as followed in Algorithm 1.

We demonstrated our system on Naver Cloud with 20 trainees and a master. However, we have also performed scalable demonstrations up to 100 users, with each trainee engaging in simulations within their Docker containers, showcasing its scalability and adaptability to any cloud platform. Moreover, the number of users (trainees) can be increased as per the requirements of the training system. This setup allows multiple trainees to engage in emulations within their Docker containers, with the master server consolidating logs for real-time oversight, ensuring a collaborative and effective cybersecurity training platform.

The Cyber5Gym platform enables single users to undertake meta-learning in 5G network cybersecurity, following initial training from a master server. This advanced, script-driven system allows users to independently control and emulate the 5G environment, including executing sophisticated cyberattacks and implementing countermeasures, through shell scripts. This capability for autonomous learning and experimentation post-training not only deepens understanding of network vulnerabilities but also equips users with the skills to adapt to and manage the evolving threats in 5G technology, ensuring continued skill enhancement in real-time cybersecurity scenarios.

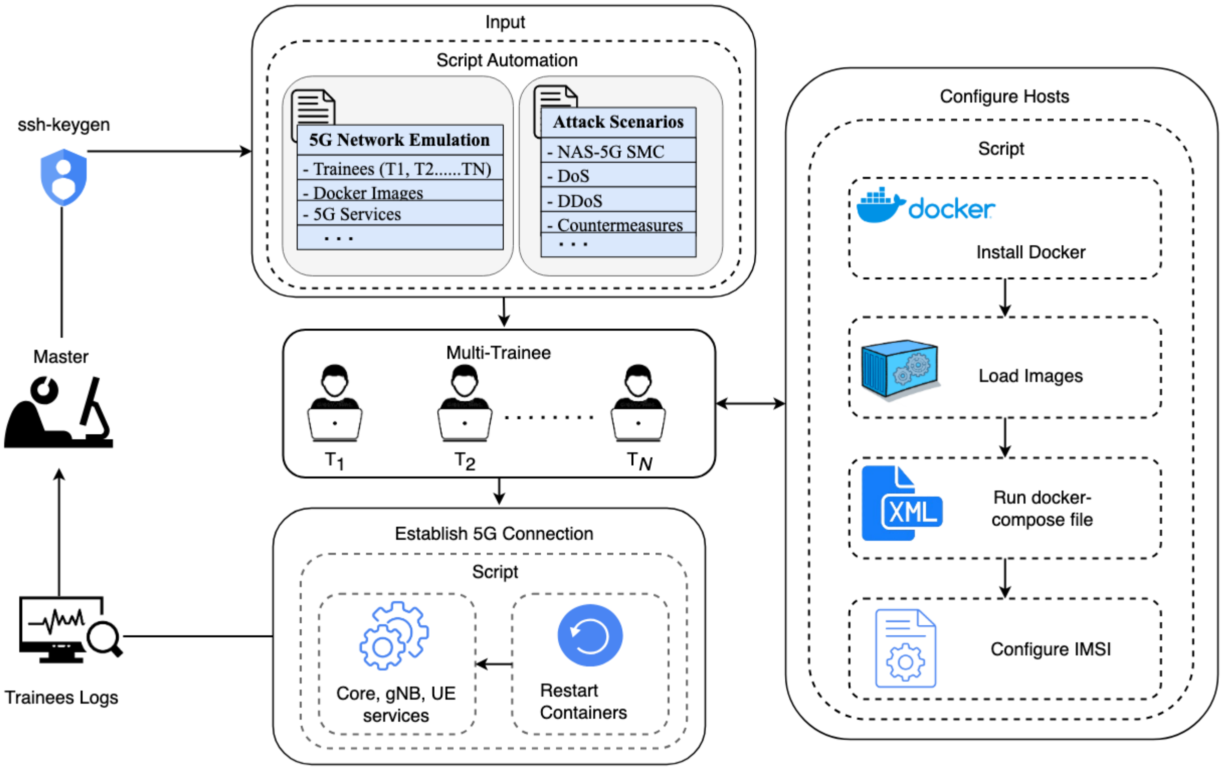
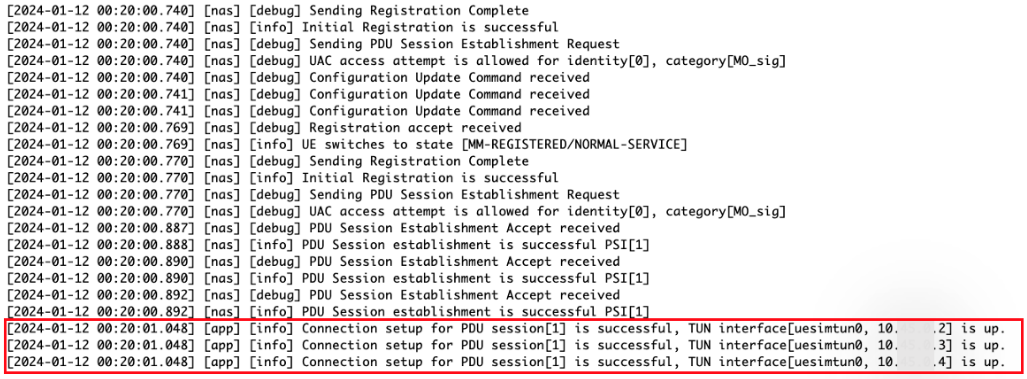


Figure 3. Workflow of a multi-user virtualized training environment setup. A master server employs ssh-keygen for secure communication with trainee instances, automates the configuration of Docker environments, initiates 5G services, and emulates a 5G network, including attacks and countermeasures. The process involves using scripts to configure trainee instances, establishing 5G connections, and managing trainee logs, ensuring a thorough training experience.



```
[2024-01-12 00:20:00.740] [nas] [debug] Sending Registration Complete
[2024-01-12 00:20:00.740] [nas] [info] Initial Registration is successful
[2024-01-12 00:20:00.740] [nas] [debug] Sending PDU Session Establishment Request
[2024-01-12 00:20:00.740] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2024-01-12 00:20:00.740] [nas] [debug] Configuration Update Command received
[2024-01-12 00:20:00.741] [nas] [debug] Configuration Update Command received
[2024-01-12 00:20:00.741] [nas] [debug] Configuration Update Command received
[2024-01-12 00:20:00.769] [nas] [debug] Registration accept received
[2024-01-12 00:20:00.769] [nas] [info] UE switches to state [MM-REGISTERED/NORMAL-SERVICE]
[2024-01-12 00:20:00.770] [nas] [debug] Sending Registration Complete
[2024-01-12 00:20:00.770] [nas] [info] Initial Registration is successful
[2024-01-12 00:20:00.770] [nas] [debug] Sending PDU Session Establishment Request
[2024-01-12 00:20:00.770] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2024-01-12 00:20:00.887] [nas] [debug] PDU Session Establishment Accept received
[2024-01-12 00:20:00.888] [nas] [info] PDU Session establishment is successful PSI[1]
[2024-01-12 00:20:00.890] [nas] [debug] PDU Session Establishment Accept received
[2024-01-12 00:20:00.890] [nas] [info] PDU Session establishment is successful PSI[1]
[2024-01-12 00:20:00.892] [nas] [debug] PDU Session Establishment Accept received
[2024-01-12 00:20:00.892] [nas] [info] PDU Session establishment is successful PSI[1]
[2024-01-12 00:20:01.048] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun0, 10.[redacted].2] is up.
[2024-01-12 00:20:01.048] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun0, 10.[redacted].3] is up.
[2024-01-12 00:20:01.048] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun0, 10.[redacted].4] is up.
```

Figure 4. 5G network establishment across distributed servers for multiple UE connectivity and active on TUN interfaces.

5.2. Demonstration: Attack Scenarios and Countermeasures

Aiming to advance the capabilities of cyber range platforms, our research is dedicated to formulating intricate scenarios that embody essential attributes such as automated deployment, robust availability, scalable frameworks, the reuse of resources, and secure isolation. This endeavor is vital for enhancing the resilience and adaptability of cyber range environments, particularly in the context of emerging 5G network technologies. By integrating Docker Containers and script-based automation, we facilitate the streamlined provisioning of services and infrastructure, thus ensuring a more efficient and agile deployment process. We deployed our system on Naver Cloud for demonstration.

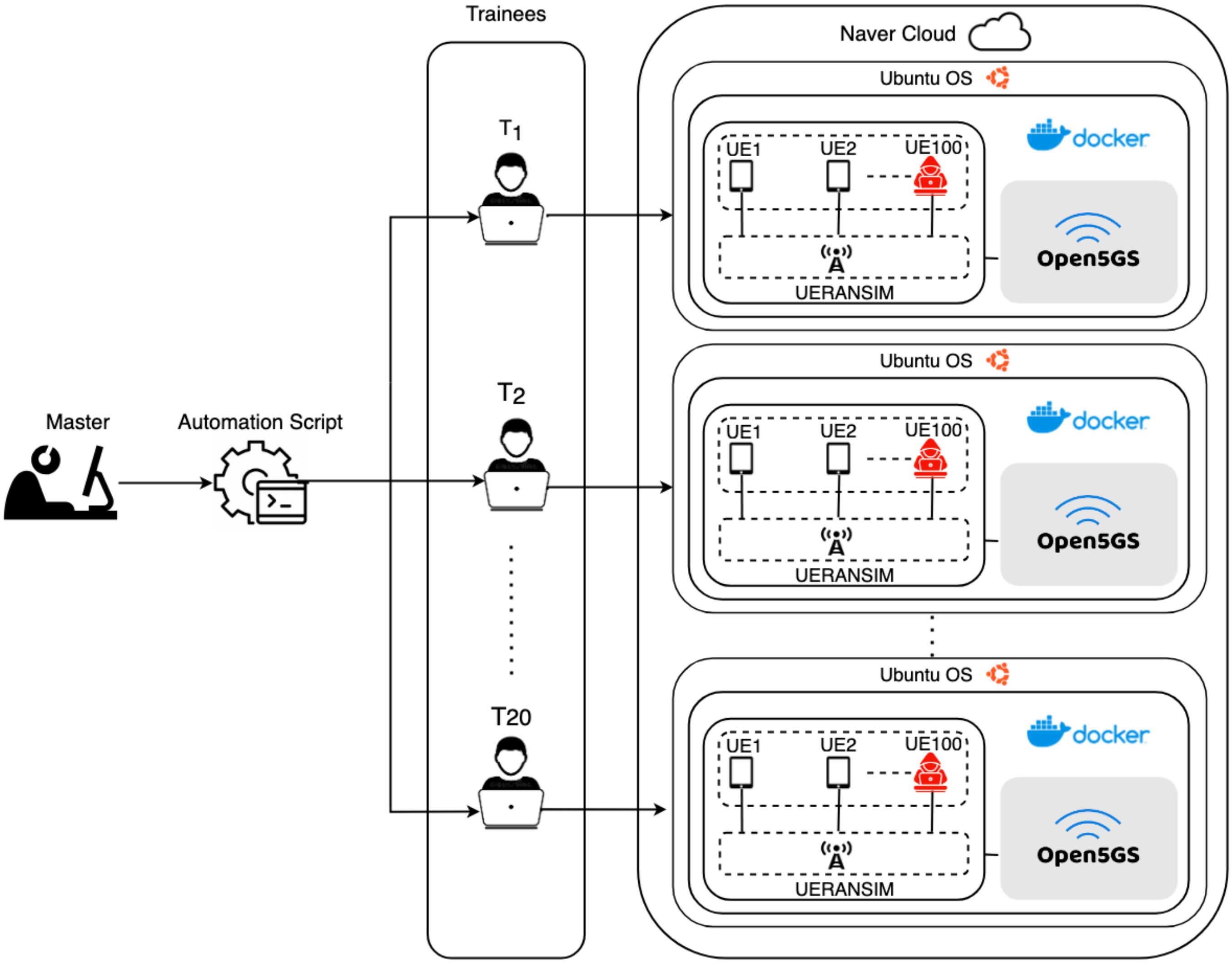


Figure 5. Architectural overview of a scalable, automated 5G network emulation platform on Naver Cloud, where a master server executes scripts to dynamically create and manage multiple instances for 20 trainees, each handling 100 UEs. This configuration provides a realistic and comprehensive training experience in 5G network operations, ensuring each trainee gains hands-on exposure to real-world network scenarios and challenges.

In this study, we focus on the security of 5G networks by examining various cyber-attack scenarios and their respective countermeasures. This section introduces different cybersecurity scenarios, each aimed at testing specific vulnerabilities in the 5G network. Using the 5Greplay [10] tool, we explore two main types of attacks: the NAS SMC Replay Attack and a high-bandwidth DoS Attack. Additionally, we include a scenario for a DDoS attack to cover a broader range of security threats.

The following content will provide detailed descriptions of each scenario, including their execution and impact on 5G networks. Alongside these attack scenarios, we also present the countermeasures developed to detect and mitigate cybersecurity threats, focusing on maintaining the stability and security of the 5G network infrastructure.

5.3. SMC Replay Attack

5.3.1. Attack Description

This attack scenario investigates the application of 5Greplay for conducting security assessments through the alteration and injection of network traffic toward specific targets. Figure 6 illustrates the NAS-5G Security Mode Command replay attack, where the configuration of 5Greplay simulates legitimate UE security messages, challenging the AMF's detection capabilities. It highlights that according to the analysis of ENISA [43] on 5G network threats, AMF components are susceptible to replay attacks, particularly of the NAS SMC procedure messages. Additionally, it references the 3GPP TS33.512 [44] specification, which suggests a test to ascertain the robustness of an AMF against such attacks.

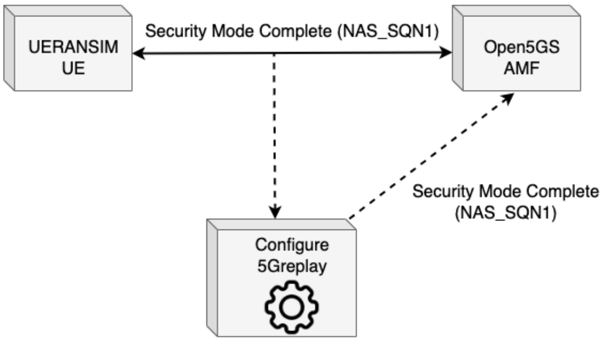


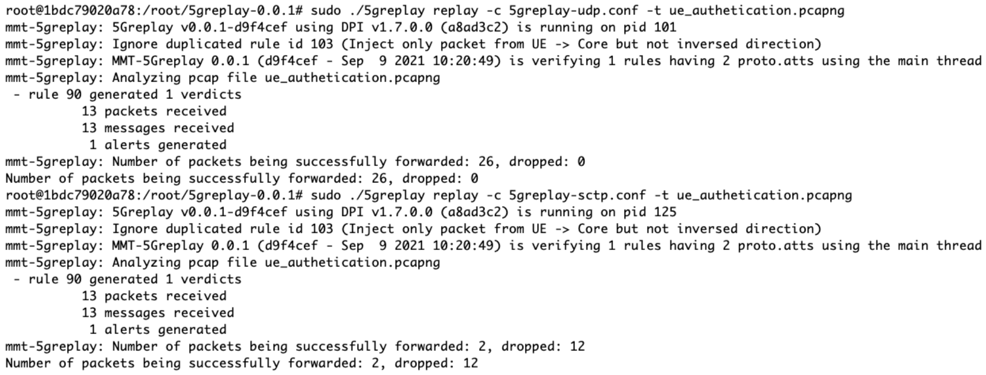
Figure 6. NAS-5G Security Mode Command replay attack.

5.3.2. Testbed Setup

The execution of this security test is carried out on a 5G emulation platform utilizing open-source tools such as Open5GS and UERANSIM. The test involves configuring 5Greplay to identify and replicate NAS-5G SMC messages sent by a UE post-authentication, assessing the online forwarding capabilities of 5Greplay and the resilience of Open5GS AMF against replay attacks.

5.3.3. Result Analysis

The implementation of the NAS SMC Replay Attack in the 5Greplay system involves the use of two specific configuration files, namely `5greplayudp.conf` and `5greplay-sctp.conf`. These files enable the testing of the attack under different network protocols. For practical testing, it is advised to begin with processing a precaptured pcap file, in this case, `ue_authentication.pcapng`, which records the authentication dialogue between a UE and AMF. This allows for the observation of the NAS SMC packet within the traffic, assessing whether the packet is correctly filtered and forwarded based on the configuration, as shown in Figure 7. The effectiveness of the filtering and forwarding rules can be further examined using tools such as Wireshark [45] or tcpdump [46], which provide a detailed view of the traffic, including the specific actions taken on the NAS SMC packet.



```
root@1bdc79020a78:/root/5greplay-0.0.1# sudo ./5greplay replay -c 5greplay-udp.conf -t ue_authetication.pcapng
mmt-5greplay: 5Greplay v0.0.1-d9f4cef using DPI v1.7.0.0 (a8ad3c2) is running on pid 101
mmt-5greplay: Ignore duplicated rule id 103 (Inject only packet from UE -> Core but not inversed direction)
mmt-5greplay: MMT-5Greplay 0.0.1 (d9f4cef - Sep  9 2021 10:20:49) is verifying 1 rules having 2 proto.atts using the main thread
mmt-5greplay: Analyzing pcap file ue_authetication.pcapng
 - rule 90 generated 1 verdicts
         13 packets received
         13 messages received
          1 alerts generated
mmt-5greplay: Number of packets being successfully forwarded: 26, dropped: 0
Number of packets being successfully forwarded: 26, dropped: 0
root@1bdc79020a78:/root/5greplay-0.0.1# sudo ./5greplay replay -c 5greplay-sctp.conf -t ue_authetication.pcapng
mmt-5greplay: 5Greplay v0.0.1-d9f4cef using DPI v1.7.0.0 (a8ad3c2) is running on pid 125
mmt-5greplay: Ignore duplicated rule id 103 (Inject only packet from UE -> Core but not inversed direction)
mmt-5greplay: MMT-5Greplay 0.0.1 (d9f4cef - Sep  9 2021 10:20:49) is verifying 1 rules having 2 proto.atts using the main thread
mmt-5greplay: Analyzing pcap file ue_authetication.pcapng
 - rule 90 generated 1 verdicts
         13 packets received
         13 messages received
          1 alerts generated
mmt-5greplay: Number of packets being successfully forwarded: 2, dropped: 12
Number of packets being successfully forwarded: 2, dropped: 12
```

Figure 7. 5Greplay logs when transmitting malicious packets to AMF component.

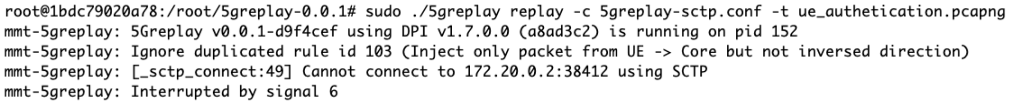
5.3.4. Implications

The NAS-5G SMC Replay attack scenario [10], carries significant implications for the security of 5G networks. This type of attack primarily exploits vulnerabilities in the AMF components of the network, where a malicious actor replays and modifies NAS

SMC procedure messages. The primary risk is the potential for unauthorized access or impersonation of a UE. This enables attackers to manipulate the security level of the connection, either by downgrading it to a weaker encryption algorithm or disabling it entirely. Such vulnerabilities lead to a wide range of security breaches, including data interception, privacy violations, and unauthorized access to network resources. In a broader sense, the successful execution of such an attack undermines trust in 5G network security, highlighting the need for robust security mechanisms and constant vigilance against emerging threats. The scenario underscores the importance of comprehensive security testing and validation tools like 5Greplay in identifying and mitigating such vulnerabilities in 5G networks.

5.3.5. Countermeasure

IP Blocking: To counter the NAS-5G SMC Replay Attack, a common measure is to block the IP address of the attacker UE. By implementing an IP filtering rule on the network firewall, incoming packets from the attacker IP can be dropped, effectively preventing the malicious traffic from reaching the network. The command `sudo iptables -A INPUT -s IP -j DROP` is used to add such a rule to the network iptables, instructing it to ignore all incoming traffic from the attacker IP address. Once these measures are implemented, any attempt to send SMC packets from the attacker UE will be thwarted as shown in Figure 8. Additionally, disabling IP broadcasts can also mitigate the risk of the network being used as an amplifier in the Internet Control Message Protocol (ICMP) Flood and Smurf attacks. However, this technique requires the deactivation of IP broadcasts across all neighboring devices to be truly effective.



```
root@1bdc79020a78:/root/5greplay-0.0.1# sudo ./5greplay replay -c 5greplay-sctp.conf -t ue_authetication.pcapng
mmt-5greplay: 5Greplay v0.0.1-d9f4cef using DPI v1.7.0.0 (a8ad3c2) is running on pid 152
mmt-5greplay: Ignore duplicated rule id 103 (Inject only packet from UE -> Core but not inversed direction)
mmt-5greplay: [_sctp_connect:49] Cannot connect to 172.20.0.2:38412 using SCTP
mmt-5greplay: Interrupted by signal 6
```

Figure 8. Attacker UE IP Blocking on 5Greplay, which results into stop traffic transmission to AMF.

5.4. DoS Attack

5.4.1. Attack Description

The 5Greplay [10] tool is designed to replay a pre-captured pcap file from a UE session intensively, to generate high-bandwidth traffic. This traffic is directed towards the 5G core service, augmenting the intensity of the simulated attack or stress test being conducted. Through the configuration of the 5Greplay tool, the attacker UE (UE 100) initiates a DoS attack by injecting a concentrated stream of high-bandwidth traffic into the network, as depicted in Figure 9. The evaluation proceeds uninterrupted until errors surface in the execution log of the target, such as the AMF, indicating possible overloading or malfunction triggered by the traffic surge.

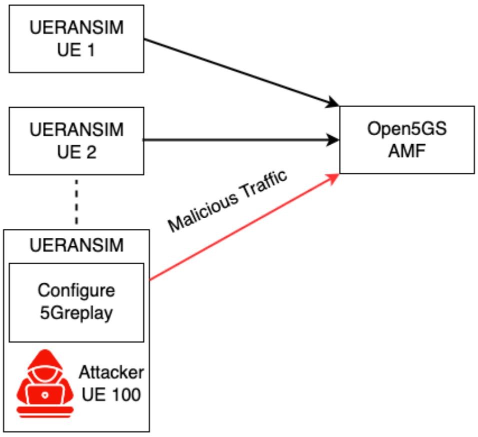


Figure 9. DoS Attack: High-bandwidth traffic injection using 5Greplay.

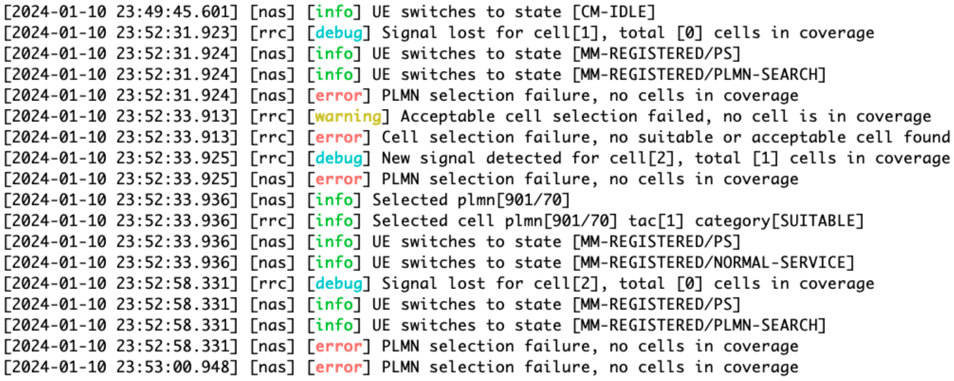
5.4.2. Testbed Setup

We assess the 5G Core Network service by replaying a pre-captured pcap file representing a complete UE session. This involves activating gNodeB with UE services, connecting to Open5GS, and then stopping the gNB and UE services. Using 5Greplay, installed on a designated UE attacker, we inject the pcap file into the Core Network services.

The configuration of 5Greplay targets specific protocols, hosts, and ports. Our attack involves replaying high-bandwidth traffic through the Stream Control Transmission Protocol (SCTP) to selected hosts and ports. Packet selection is based on the IP address of the UERANSIM UE and an SCTP destination port used by the Next Generation Application Protocol (NGAP), focusing solely on SCTP data chunks. We progressively increase the attack intensity by augmenting the number of packet copies and evaluating the ability of the network to manage surges in data traffic.

5.4.3. Result Analysis

The analysis of Open5GS AMF logs post-injection of high-bandwidth traffic through UE revealed that the AMF components experienced a crash after replaying the traffic (see Figure 10). This crash was attributed to the failure of the AMF to decode Next Generation Application Protocol (NGAP) messages, indicating a significant decoding challenge that could disrupt protocol communication with other network components. Further, warnings about Abstract Syntax Notation One—Protocol Data Unit (ASN-PDU) and NGAP-PDU (Protocol Data Unit) decoding failures point to potential misinterpretation or corruption in the protocol data units, leading to possible erroneous network behaviors.



```
[2024-01-10 23:49:45.601] [nas] [info] UE switches to state [CM-IDLE]
[2024-01-10 23:52:31.923] [rrc] [debug] Signal lost for cell[1], total [0] cells in coverage
[2024-01-10 23:52:31.924] [nas] [info] UE switches to state [MM-REGISTERED/PS]
[2024-01-10 23:52:31.924] [nas] [info] UE switches to state [MM-REGISTERED/PLMN-SEARCH]
[2024-01-10 23:52:31.924] [nas] [error] PLMN selection failure, no cells in coverage
[2024-01-10 23:52:33.913] [rrc] [warning] Acceptable cell selection failed, no cell is in coverage
[2024-01-10 23:52:33.913] [rrc] [error] Cell selection failure, no suitable or acceptable cell found
[2024-01-10 23:52:33.925] [rrc] [debug] New signal detected for cell[2], total [1] cells in coverage
[2024-01-10 23:52:33.925] [nas] [error] PLMN selection failure, no cells in coverage
[2024-01-10 23:52:33.936] [nas] [info] Selected plmn[901/70]
[2024-01-10 23:52:33.936] [rrc] [info] Selected cell plmn[901/70] tac[1] category[SUITABLE]
[2024-01-10 23:52:33.936] [nas] [info] UE switches to state [MM-REGISTERED/PS]
[2024-01-10 23:52:33.936] [nas] [info] UE switches to state [MM-REGISTERED/NORMAL-SERVICE]
[2024-01-10 23:52:58.331] [rrc] [debug] Signal lost for cell[2], total [0] cells in coverage
[2024-01-10 23:52:58.331] [nas] [info] UE switches to state [MM-REGISTERED/PS]
[2024-01-10 23:52:58.331] [nas] [info] UE switches to state [MM-REGISTERED/PLMN-SEARCH]
[2024-01-10 23:52:58.331] [nas] [error] PLMN selection failure, no cells in coverage
[2024-01-10 23:53:00.948] [nas] [error] PLMN selection failure, no cells in coverage
```

Figure 10. DoS attack targeting 5G network connectivity has disrupted victim UEs connectivity, leading to issues in AMF and causing failures in Public Land Mobile Network (PLMN) selection, resulting in network instability.

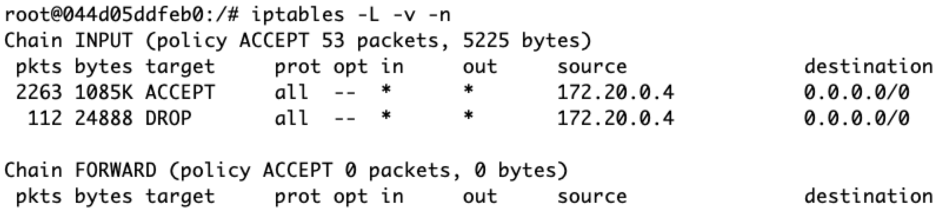
Concurrently, upon the attack execution, all UEs connected to the AMF reported errors, signifying the extensive impact of the attacker UE on the network. The high-bandwidth traffic attack resulted in network connectivity disruptions and delays for the UEs. As the situation escalated, UEs attempting to re-establish connection faced Public Land Mobile Network (PLMN) selection failures and changes in state, struggling to find a cell for connection in their coverage area. This led to repeated connection attempts and challenges in maintaining network stability, highlighting the critical need for enhanced mechanisms in 5G Core Network services to effectively handle surges in data traffic and safeguard network reliability.

5.4.4. Implications

The observed crashes in Open5GS AMF following high-bandwidth traffic injections highlight a crucial vulnerability in 5G networks (see Figure 10). The inability of AMF to decode NGAP messages under such conditions suggests a risk of protocol communication breakdowns with other network elements. The errors reported by all UEs connected to the AMF during the attack further underscore the widespread consequences of such disruptions. These findings emphasize the urgent need for robust mechanisms in 5G core services to handle traffic surges and ensure network reliability, especially in managing data traffic peaks and maintaining consistent network connectivity.

5.4.5. Countermeasures

Rate Limiting: In fortifying our 5G network against high-bandwidth threats, we establish a rate limit of 500 kb/s. This threshold is chosen to balance efficient data flow with the prevention of network overloads, particularly in high-traffic scenarios. The implementation involves configuring iptables to monitor and control the data flow from the IP of attacker UE. Integrating a hashlimit module is pivotal in this setup, as it regulates bandwidth to ensure traffic adheres to the set threshold, thereby automatically rejecting any excess packets. Figure 11 shows the effective implementation of rate limiting in iptables, demonstrating the strengthened defenses of the system against a DoS attack to drop 24,888 byes along with 112 packets that exceed 500 kb/s. Implementing a rate limit is a crucial step in enhancing the performance and security of 5G networks, effectively managing high-bandwidth traffic, and ensuring network stability.

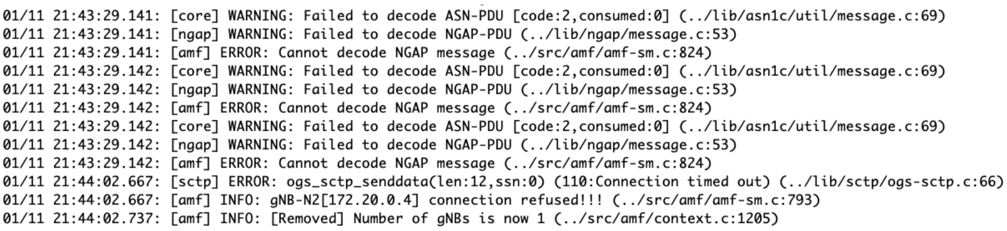


```
root@044d05ddfeb0:/# iptables -L -v -n
Chain INPUT (policy ACCEPT 53 packets, 5225 bytes)
 pkts bytes target     prot opt in     out     source               destination
 2263 1085K ACCEPT     all  --  *      *       172.20.0.4           0.0.0.0/0
  112 24888 DROP       all  --  *      *       172.20.0.4           0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Figure 11. Applying rate limiting results in packet 112 dropped for exceeding the 500 kb/s speed limit in response to a DoS attack.

IP Blocking: The iptables employ a firewall mechanism to block incoming packets from the IP of attacker UE. This setup effectively drops any packets originating from this source, serving as a critical line of defense against potential network threats. Through continuous monitoring, we observe that the iptables configuration consistently rejects traffic from the attacker UE, leading to their disconnection from the RAN and stopping AMF services. This action plays a pivotal role in upholding the security and integrity of our 5G network infrastructure. Figure 12 depicts the system logs following IP blocking, a decisive countermeasure against a DoS attack, illustrating the disruption and subsequent refusal of malicious UE connections.



```
01/11 21:43:29.141: [core] WARNING: Failed to decode ASN-PDU [code:2,consumed:0] (../lib/asn1c/util/message.c:69)
01/11 21:43:29.141: [ngap] WARNING: Failed to decode NGAP-PDU (../lib/ngap/message.c:53)
01/11 21:43:29.141: [amf] ERROR: Cannot decode NGAP message (../src/amf/amf-sm.c:824)
01/11 21:43:29.142: [core] WARNING: Failed to decode ASN-PDU [code:2,consumed:0] (../lib/asn1c/util/message.c:69)
01/11 21:43:29.142: [ngap] WARNING: Failed to decode NGAP-PDU (../lib/ngap/message.c:53)
01/11 21:43:29.142: [amf] ERROR: Cannot decode NGAP message (../src/amf/amf-sm.c:824)
01/11 21:43:29.142: [core] WARNING: Failed to decode ASN-PDU [code:2,consumed:0] (../lib/asn1c/util/message.c:69)
01/11 21:43:29.142: [ngap] WARNING: Failed to decode NGAP-PDU (../lib/ngap/message.c:53)
01/11 21:43:29.142: [amf] ERROR: Cannot decode NGAP message (../src/amf/amf-sm.c:824)
01/11 21:44:02.667: [sctp] ERROR: ogs_sctp_senddata(len:12,ssn:0) (110:Connection timed out) (../lib/sctp/ogs-sctp.c:66)
01/11 21:44:02.667: [amf] INFO: gNB-N2[172.20.0.4] connection refused!!! (../src/amf/amf-sm.c:793)
01/11 21:44:02.737: [amf] INFO: [Removed] Number of gNBs is now 1 (../src/amf/context.c:1205)
```

Figure 12. Mitigating DoS attack by implementing IP blocking on the attacker UE.

5.5. DDoS Attack

5.5.1. Attacks Description

A Distributed Denial-of-Service (DDoS) attack is designed to flood network resources and target the 5G CN component AMF. The attack is executed using multiple UEs, including both victim and attacker UEs. The attacker UE is configured to simulate a large number of UEs (i.e., 350), creating an excessive load on network resources. This configuration leads to continuous connection attempts to the AMF by all simulated UEs, effectively emulating a DDoS attack. The aim is to assess the impact on CN services and their ability to handle such demanding traffic scenarios. Figure 13 depicts the DDoS scenario, highlighting the flow of malicious traffic from a multitude of counterfeit UEs, including the attacker UE, to the Open5GS AMF. This illustration demonstrates the scale of the attack, with the AMF being the focal point of excessive connection requests, which are indicative of the attack's intent to overload system resources.

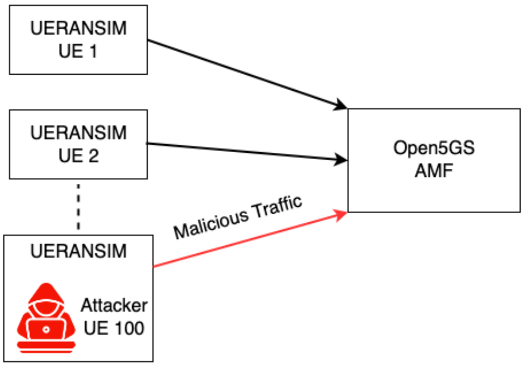


Figure 13. Representation of DDoS attack by emulating 350 Counterfeit UEs to overload system resources.

5.5.2. Testbed Setup

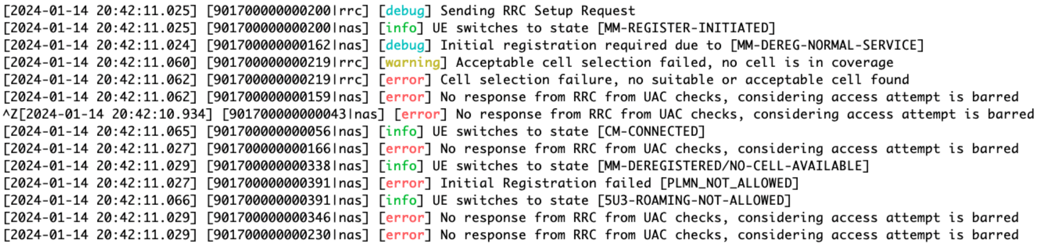
The testbed includes executing the DDoS attack in our 5G system and involves a detailed, sequential approach. Initially, the setup requires the activation of victim UEs. This is achieved by starting both their respective gNB and UE services, and establishing their presence in the network.

Following the activation of the victim UEs, the next step is to execute the attacker UE. This is a critical phase where the attacker UE is programmed to simulate the behavior of 350 UEs. The goal of this emulation is to create a significant load on the network resources, particularly targeting the victim UEs and AMF. To initiate this attack, the attacker UE persistently endeavors to establish connections with the AMF. This approach entails not only overwhelming the AMF with an excessive number of connection requests but also significantly depleting network resources.

5.5.3. Result Analysis

The DDoS attack, initiated by the attacker UE, has significant implications for the network, which leads to two primary consequences for the network. First, it results in network connection interruptions for the victim UEs, hindering their communication capabilities within the network. Second, it induces connectivity delays for these UEs, negatively impacting data transmission speed and overall network efficiency.

Figure 14 logs show key disruptions, such as cell selection failure, indicating the network inability to connect devices to a cell during a DDoS attack, and No response from Radio Resource Control (RRC), highlighting a breakdown in communication between devices and the network control units. These errors are representative of a network under cyberattack, where normal operations are compromised, leading to failed connections and communication breakdowns within the 5G network.



```
[2024-01-14 20:42:11.025] [901700000000200|rrc] [debug] Sending RRC Setup Request
[2024-01-14 20:42:11.025] [901700000000200|nas] [info] UE switches to state [MM-REGISTER-INITIATED]
[2024-01-14 20:42:11.024] [901700000000162|nas] [debug] Initial registration required due to [MM-DEREG-NORMAL-SERVICE]
[2024-01-14 20:42:11.060] [901700000000219|rrc] [warning] Acceptable cell selection failed, no cell is in coverage
[2024-01-14 20:42:11.062] [901700000000219|rrc] [error] Cell selection failure, no suitable or acceptable cell found
[2024-01-14 20:42:11.062] [901700000000159|nas] [error] No response from RRC from UAC checks, considering access attempt is barred
^Z[2024-01-14 20:42:10.934] [901700000000043|nas] [error] No response from RRC from UAC checks, considering access attempt is barred
[2024-01-14 20:42:11.065] [901700000000056|nas] [info] UE switches to state [CM-CONNECTED]
[2024-01-14 20:42:11.027] [901700000000166|nas] [error] No response from RRC from UAC checks, considering access attempt is barred
[2024-01-14 20:42:11.029] [901700000000338|nas] [info] UE switches to state [MM-DEREGISTERED/NO-CELL-AVAILABLE]
[2024-01-14 20:42:11.027] [901700000000391|nas] [error] Initial Registration failed [PLMN_NOT_ALLOWED]
[2024-01-14 20:42:11.066] [901700000000391|nas] [info] UE switches to state [5U3-ROAMING-NOT-ALLOWED]
[2024-01-14 20:42:11.029] [901700000000346|nas] [error] No response from RRC from UAC checks, considering access attempt is barred
[2024-01-14 20:42:11.029] [901700000000230|nas] [error] No response from RRC from UAC checks, considering access attempt is barred
```

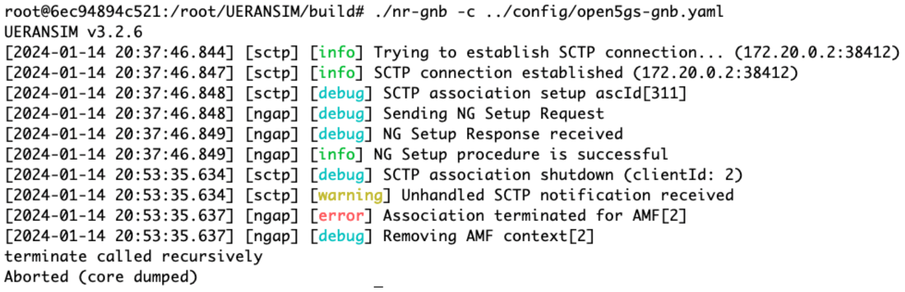
Figure 14. System logs depicting a DDoS attack scenario in a 5G network. The logs demonstrate various errors and warning messages, including failed cell selection and access attempt barring, indicative of the network response to the emulated cyberattack.

5.5.4. Implications

The impact of such an attack goes beyond direct network disturbances. In heavily populated urban centers, especially during peak times, its widespread effects could cause major service disruptions and significant risks to data integrity [47]. Economically, the implications are profound, potentially leading to substantial financial losses for businesses and consumers heavily reliant on 5G connectivity [48,49]. The attack also heightens security risks, increasing the likelihood of unauthorized access, data breaches, and network service disruptions [50].

5.5.5. Countermeasures

IP Blocking: Implementing IP blocking is a crucial strategy in mitigating DDoS attacks on 5G networks. This method focuses on identifying and subsequently blocking access from the malicious IP address of attacker UE using iptables. By preventing these identified sources from accessing the network, IP blocking not only stops ongoing attacks but also acts as a preventive measure against future attacks from the same origins. This approach is vital for safeguarding the network against unauthorized access and ensuring continuous, secure network operations. Figure 15 depicts logs where a gNB connection is forcibly terminated from the AMF, a key countermeasure in the context of a DDoS attack. This termination, indicated by messages such as Association terminated for AMF [2], signifies the disruption of an attacker UE connection, showcasing an effective defensive strategy in the network security protocol.



```
root@6ec94894c521:/root/UERANSIM/build# ./nr-gnb -c ../config/open5gs-gnb.yaml
UERANSIM v3.2.6
[2024-01-14 20:37:46.844] [sctp] [info] Trying to establish SCTP connection... (172.20.0.2:38412)
[2024-01-14 20:37:46.847] [sctp] [info] SCTP connection established (172.20.0.2:38412)
[2024-01-14 20:37:46.848] [sctp] [debug] SCTP association setup ascId[311]
[2024-01-14 20:37:46.848] [ngap] [debug] Sending NG Setup Request
[2024-01-14 20:37:46.849] [ngap] [debug] NG Setup Response received
[2024-01-14 20:37:46.849] [ngap] [info] NG Setup procedure is successful
[2024-01-14 20:53:35.634] [sctp] [debug] SCTP association shutdown (clientId: 2)
[2024-01-14 20:53:35.634] [sctp] [warning] Unhandled SCTP notification received
[2024-01-14 20:53:35.637] [ngap] [error] Association terminated for AMF[2]
[2024-01-14 20:53:35.637] [ngap] [debug] Removing AMF context[2]
terminate called recursively
Aborted (core dumped)
```

Figure 15. System logs demonstrating the termination of a gNB connection from the AMF as a response to a DDoS attack in a 5G network.

Regulating Concurrent Users: One effective countermeasure against DDoS attacks in 5G networks involves controlling the number of concurrent users, or UEs. By managing the number of active UEs at any given time, the network can more effectively allocate and manage its resources. This regulation helps reduce the likelihood of the network becoming overwhelmed during a DDoS attack, thereby maintaining stability and performance.

6. Discussion

The development and implementation of the Cyber5Gym framework represent significant strides toward addressing the complex cybersecurity challenges inherent in emerging 5G networks. By simulating real-world attack scenarios and defensive strategies within a dynamic training environment, Cyber5Gym provides a foundational platform for cybersecurity professionals to hone their skills. However, as we navigate through the limitations and potential enhancements of the system, several critical discussion points emerge that are pivotal for its future development and effectiveness.

The reliance on SSH for task automation and script execution can be seen as a manual and less scalable approach. While effective for smaller environments, this method may not be optimal for larger, more dynamic settings where scalability and flexibility are crucial. Integrating Kubernetes could overcome this limitation by offering a robust and scalable orchestration platform that could significantly enhance the management of containerized applications and services. This would enable the facilitation of more complex and dynamic training scenarios, thereby improving both efficiency and reliability. This evolution is essential for accommodating larger groups of trainees (e.g., hundreds of trainees) and more sophisticated simulation requirements. Aside from this, the assessment of the Cyber5Gym training's effectiveness and scalability in real-world applications presents a notable challenge, particularly due to the involvement of human trainees and the need to simulate real-world scenarios across hundreds of systems, which could be potentially costly and complex.

Additionally, the exclusive use of Docker for virtualization, despite its efficiency and ease of deployment, introduces performance constraints and potential security vulnerabilities. For instance, in large-scale environments, it may not adequately represent the complex interactions between network elements in scenarios involving extensive trainee participation. The shared kernel architecture of Docker containers raises security concerns, particularly in simulations of cyberattack scenarios that target kernel-level vulnerabilities. This underscores the necessity of exploring additional virtualization technologies or hybrid models for future work that combine the strengths of Docker with other virtualization or container management solutions. The hybrid model virtualization would also enhance the efficiency of the training system to run diverse attack scenarios concurrently across multiple trainee systems, a feature essential for preparing cybersecurity professionals for the realities of multifaceted or simultaneous cyber threats.

For future enhancements, we plan to evaluate the effectiveness of the Cyber5Gym training through hands-on training sessions involving human trainees. By collecting feedback and precisely measuring the accuracy of operational execution through trainee logs, we aim to gain a comprehensive understanding of the system's impact on improving cybersecurity skills. Moreover, cybersecurity training at Cyber5Gym focuses on standard or foundational security attack scenarios, which is vital for laying the groundwork in cybersecurity training for 5G networks. This fundamental approach establishes an essential understanding of cybersecurity threats and defenses. Nonetheless, the rapid evolution of the 5G technology landscape introduces increasingly novel threats that exploit the distinct vulnerabilities of 5G infrastructure. To remain effective, our system must keep evolving to incorporate these advanced threats, ensuring that cybersecurity professionals are adequately equipped to address the challenges posed by the ever-changing cybersecurity landscape. This discussion underscores the imperative need for ongoing development and adaptation of the Cyber5Gym system to keep pace with the rapidly evolving 5G cybersecurity landscape. By addressing the current limitations and actively incorporating advancements in technology and threat simulation, Cyber5Gym can significantly enhance its contribution to the field of cybersecurity training.

7. Conclusions

In this paper, we present the Cyber5Gym system, designed to fill the gap in automated and virtualized cybersecurity training for 5G networks, with an emphasis on ensuring flexibility, resource efficiency, and scalability. We have effectively demonstrated the efficacy of our system in emulating realistic 5G network environments for multi-users (e.g., a master server and trainees) utilizing Open5GS, UERANSIM, and automation of both attack scenarios and their countermeasures in a cloud-based environment. This approach significantly improves the practicality and effectiveness of cybersecurity training, enabling a dynamic adaptation to diverse cyber threats. The use of open-source tools in our system ensures reproducibility and facilitates further research and development of cybersecurity training systems for 5G networks. This aspect significantly enhances the practicality of the training system and its adaptability to various cyber threats.

Despite the system's innovative approach, assessing the effectiveness and scalability of the Cyber5Gym training in real-world applications remains challenging, as it involves human trainees and hundreds of systems to simulate real-world scenarios, which could be potentially costly and complex. Moreover, the reliance of our framework on SSH for task automation may not scale well in larger environments. The Cyber5Gym's focus on standard security attack scenarios, although crucial for establishing a baseline understanding of cybersecurity threats and defenses, needs to evolve. This evolution is essential for ensuring that cybersecurity professionals are well-prepared to tackle the challenges posed by the constantly changing cybersecurity landscape.

For future enhancements, we aim to integrate Kubernetes to further streamline the automation processes in the Cyber5Gym. We plan to evaluate the effectiveness of the Cyber5Gym training by involving human trainees in hands-on training sessions, collecting their feedback, and precisely measuring the accuracy of operational execution through analysis of trainee logs to ensure a comprehensive understanding of the impact of the system on improving cybersecurity skills. We also plan to enhance the training system by (i) enriching the system with a broader spectrum of attack scenarios, including RRC Reply Attack [5], Eavesdropping [5], and NAS Manipulation [7], and (ii) executing different attack scenarios at each of the trainee systems simultaneously, each accompanied by relevant countermeasures. This advancement aims to further enhance the capabilities of cybersecurity professionals to safeguard 5G infrastructures, thereby contributing to the resilience and security of these critical networks.

Author Contributions: Conceptualization, M.A.H., U.E. and H.-c.K.; methodology, M.A.H., U.E. and H.-c.K.; software, M.A.H. and U.E.; validation, M.A.H. and U.E.; formal analysis, M.A.H., U.E. and H.-c.K.; investigation, M.A.H., U.E. and H.-c.K.; resources, H.-c.K.; data curation, M.A.H. and U.E.; writing—original draft preparation, M.A.H. and U.E.; writing—review and editing, M.A.H., U.E. and H.-c.K.; visualization, U.E, M.A.H. and H.-c.K.; supervision, H.-c.K.; project administration, H.-c.K.; funding acquisition, H.-c.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by a 2021 Research Grant from Sangmyung University, South Korea.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

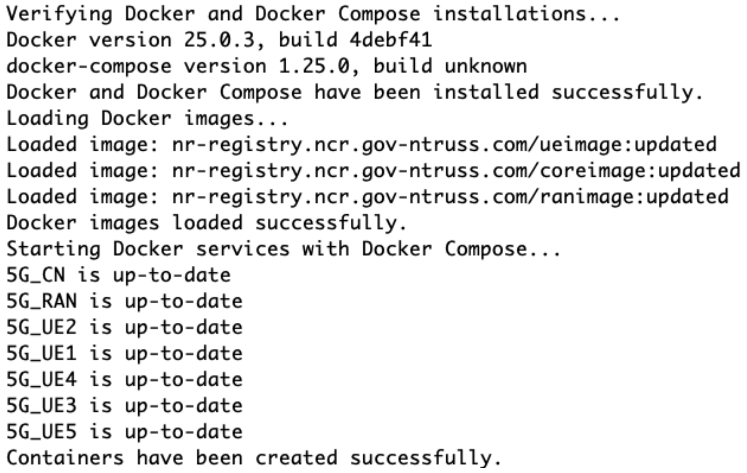
Abbreviations

The following abbreviations are used in this manuscript:

UE	User Equipment
RAN	Radio Access Network
CN	Core Network
AMF	Access and Mobility Management Function
SMF	Session Management Function
UPF	User Plane Function
SMC	Security Mode Complete
NAS	Non-Access Stratum
DoS	Denial of Service
DDoS	Distributed Denial of Service
LTE	Long-Term Evolution
EPC	Evolved Packet Core
PLMN	Public Land Mobile Network
NGAP	Next Generation Application Protocol
MIMO	Multiple Input Multiple Output
RRC	Radio Resource Control
IoT	Internet of Things
VM	Virtual Machine
FSM	Finite State Machine

Appendix A. Trainees System Configuration

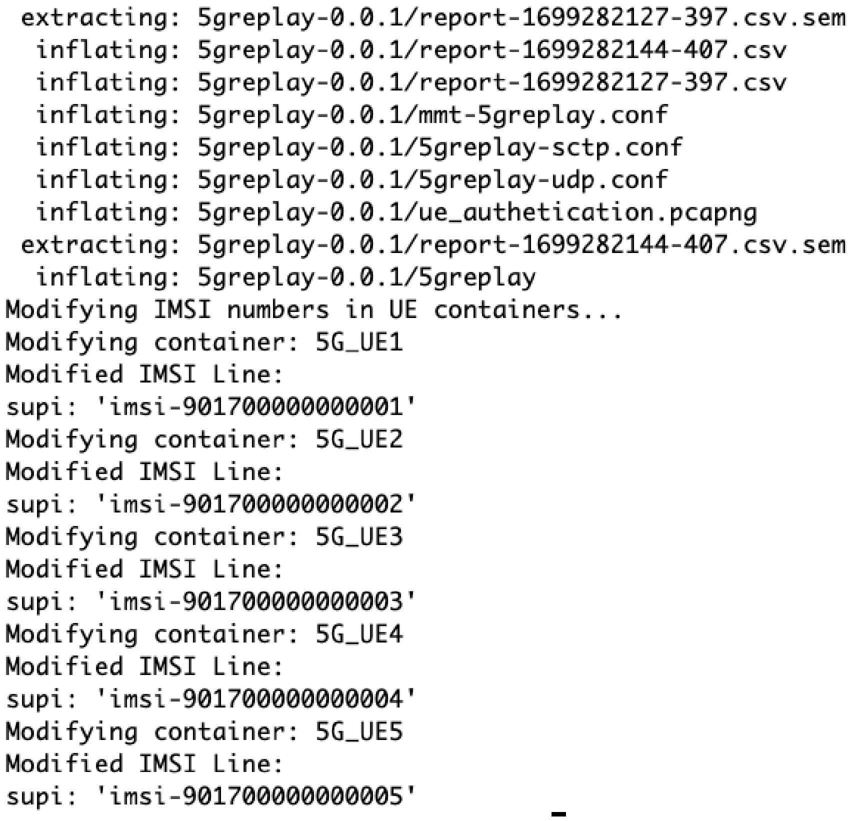
The execution of a dedicated script facilitates the systematic establishment of the 5G network emulation across host servers. This script installs Docker and its dependencies, a foundational step for the subsequent loading of the core, ran, and ue Docker images as illustrated in Figure A1. The automated provisioning of these elements is integral to the emulation's infrastructure.



```
Verifying Docker and Docker Compose installations...
Docker version 25.0.3, build 4debf41
docker-compose version 1.25.0, build unknown
Docker and Docker Compose have been installed successfully.
Loading Docker images...
Loaded image: nr-registry.ncr.gov-ntruss.com/ueimage:updated
Loaded image: nr-registry.ncr.gov-ntruss.com/coreimage:updated
Loaded image: nr-registry.ncr.gov-ntruss.com/ranimage:updated
Docker images loaded successfully.
Starting Docker services with Docker Compose...
5G_CN is up-to-date
5G_RAN is up-to-date
5G_UE2 is up-to-date
5G_UE1 is up-to-date
5G_UE4 is up-to-date
5G_UE3 is up-to-date
5G_UE5 is up-to-date
Containers have been created successfully.
```

Figure A1. Installation of Docker and Docker Compose, loading of network component images, and creation of core, RAN, and UE containers for the 5G emulation setup.

Following the setup of Docker, the script utilizes Docker Compose to initiate the necessary services that comprise the 5G network and dynamic creation of multiple UEs. Figure A2 intricacies of UE configuration are addressed by the script, which sets unique IMSI values for each UE instance, ensuring proper identification within the network. Furthermore, one of the UE instances is configured with 5Greplay, a tool for simulating network traffic and testing the network's resilience against replay attacks.

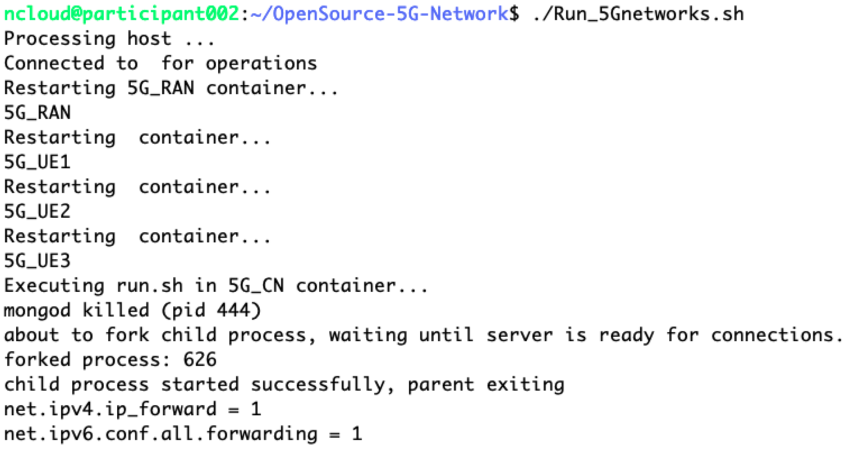


```
 extracting: 5greplay-0.0.1/report-1699282127-397.csv.sem
  inflating: 5greplay-0.0.1/report-1699282144-407.csv
  inflating: 5greplay-0.0.1/report-1699282127-397.csv
  inflating: 5greplay-0.0.1/mmt-5greplay.conf
  inflating: 5greplay-0.0.1/5greplay-sctp.conf
  inflating: 5greplay-0.0.1/5greplay-udp.conf
  inflating: 5greplay-0.0.1/ue_authetication.pcapng
 extracting: 5greplay-0.0.1/report-1699282144-407.csv.sem
  inflating: 5greplay-0.0.1/5greplay
Modifying IMSI numbers in UE containers...
Modifying container: 5G_UE1
Modified IMSI Line:
supi: 'imsi-901700000000001'
Modifying container: 5G_UE2
Modified IMSI Line:
supi: 'imsi-901700000000002'
Modifying container: 5G_UE3
Modified IMSI Line:
supi: 'imsi-901700000000003'
Modifying container: 5G_UE4
Modified IMSI Line:
supi: 'imsi-901700000000004'
Modifying container: 5G_UE5
Modified IMSI Line:
supi: 'imsi-901700000000005'
```

Figure A2. Configuration of 5Greplay and IMSI numbers for UE containers in the 5G network emulation.

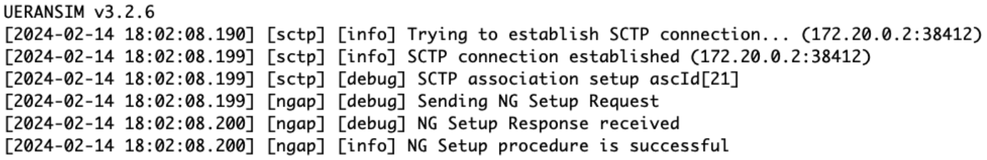
Appendix B. 5G Network Emulation

We provide a comprehensive view of the orchestrated processes undertaken by the master server to establish the emulated 5G network as depicted in Figures A3–A6. The master server commences by forming connections with each host within the trainee system, a prerequisite for the network setup. MongoDB services are then initiated, essential for database management and session handling, followed by the activation of IP forwarding to facilitate inter-network communication. The progression continues with the launch of gNodeB services, essential for radio network signaling and interfacing. Once gNB is operational, the setup proceeds with the initiation of User Equipment services. The final phase of the setup involves configuring the 'uesimtun0' network interface, a critical component for UE connectivity and data transmission within the emulated environment.



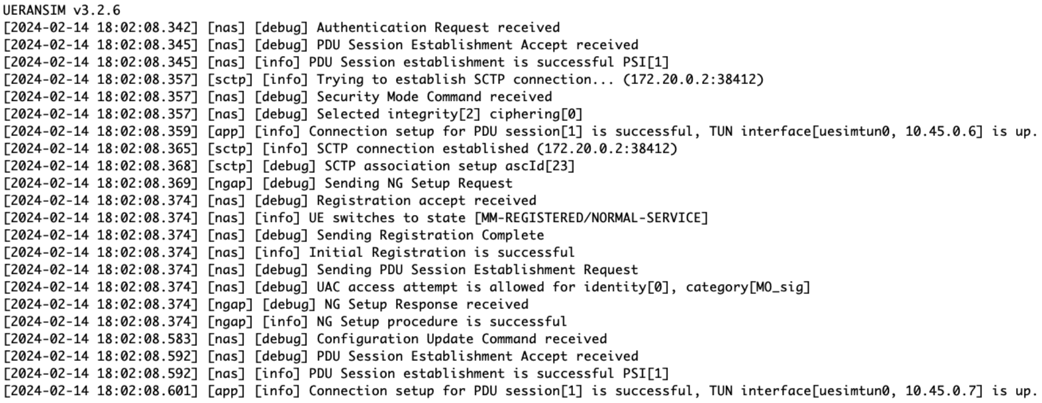
```
ncloud@participant002:~/OpenSource-5G-Network$ ./Run_5Gnetworks.sh
Processing host ...
Connected to  for operations
Restarting 5G_RAN container...
5G_RAN
Restarting  container...
5G_UE1
Restarting  container...
5G_UE2
Restarting  container...
5G_UE3
Executing run.sh in 5G_CN container...
mongod killed (pid 444)
about to fork child process, waiting until server is ready for connections.
forked process: 626
child process started successfully, parent exiting
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
```

Figure A3. Initialization of MongoDB services and IP forwarding in core network.



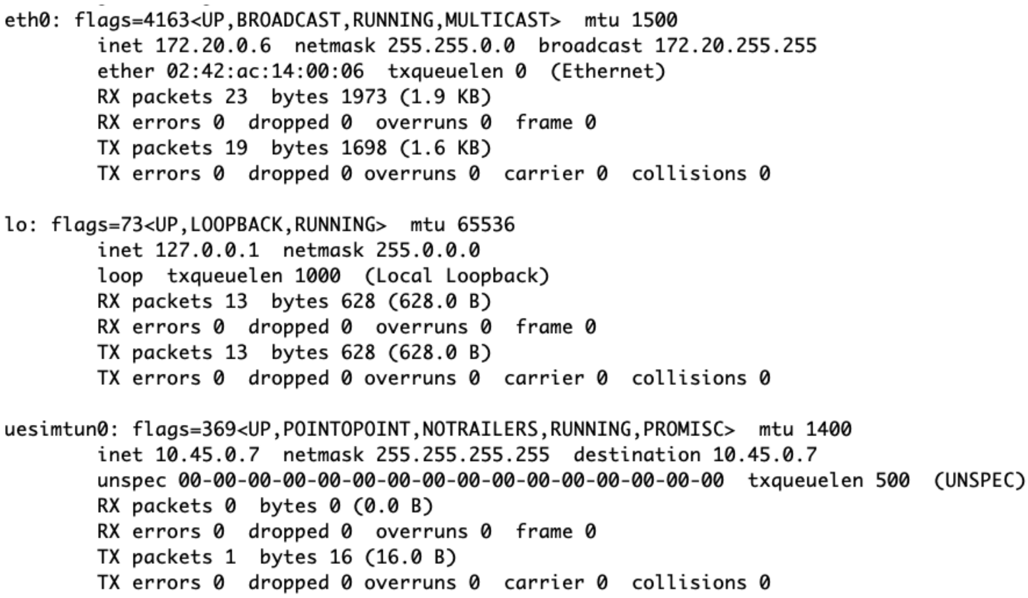
```
UERANSIM v3.2.6
[2024-02-14 18:02:08.190] [sctp] [info] Trying to establish SCTP connection... (172.20.0.2:38412)
[2024-02-14 18:02:08.199] [sctp] [info] SCTP connection established (172.20.0.2:38412)
[2024-02-14 18:02:08.199] [sctp] [debug] SCTP association setup ascId[21]
[2024-02-14 18:02:08.199] [ngap] [debug] Sending NG Setup Request
[2024-02-14 18:02:08.200] [ngap] [debug] NG Setup Response received
[2024-02-14 18:02:08.200] [ngap] [info] NG Setup procedure is successful
```

Figure A4. SCTP connection establishment and NG setup for gNB in the 5G network emulation.



```
UERANSIM v3.2.6
[2024-02-14 18:02:08.342] [nas] [debug] Authentication Request received
[2024-02-14 18:02:08.345] [nas] [debug] PDU Session Establishment Accept received
[2024-02-14 18:02:08.345] [nas] [info] PDU Session establishment is successful PSI[1]
[2024-02-14 18:02:08.357] [sctp] [info] Trying to establish SCTP connection... (172.20.0.2:38412)
[2024-02-14 18:02:08.357] [nas] [debug] Security Mode Command received
[2024-02-14 18:02:08.357] [nas] [debug] Selected integrity[2] ciphering[0]
[2024-02-14 18:02:08.359] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun0, 10.45.0.6] is up.
[2024-02-14 18:02:08.365] [sctp] [info] SCTP connection established (172.20.0.2:38412)
[2024-02-14 18:02:08.368] [sctp] [debug] SCTP association setup ascId[23]
[2024-02-14 18:02:08.369] [ngap] [debug] Sending NG Setup Request
[2024-02-14 18:02:08.374] [nas] [debug] Registration accept received
[2024-02-14 18:02:08.374] [nas] [info] UE switches to state [MM-REGISTERED/NORMAL-SERVICE]
[2024-02-14 18:02:08.374] [nas] [debug] Sending Registration Complete
[2024-02-14 18:02:08.374] [nas] [info] Initial Registration is successful
[2024-02-14 18:02:08.374] [nas] [debug] Sending PDU Session Establishment Request
[2024-02-14 18:02:08.374] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2024-02-14 18:02:08.374] [ngap] [debug] NG Setup Response received
[2024-02-14 18:02:08.374] [ngap] [info] NG Setup procedure is successful
[2024-02-14 18:02:08.583] [nas] [debug] Configuration Update Command received
[2024-02-14 18:02:08.592] [nas] [debug] PDU Session Establishment Accept received
[2024-02-14 18:02:08.592] [nas] [info] PDU Session establishment is successful PSI[1]
[2024-02-14 18:02:08.601] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun0, 10.45.0.7] is up.
```

Figure A5. Log overview of multiple user equipment services initialization and PDU session establishment in trainees system.



```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.0.6  netmask 255.255.0.0  broadcast 172.20.255.255
        ether 02:42:ac:14:00:06  txqueuelen 0  (Ethernet)
        RX packets 23  bytes 1973 (1.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 1698 (1.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 13  bytes 628 (628.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 628 (628.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

uesimtun0: flags=369<UP,POINTOPOINT,NOTRAILERS,RUNNING,PROMISC>  mtu 1400
        inet 10.45.0.7  netmask 255.255.255.255  destination 10.45.0.7
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1  bytes 16 (16.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure A6. UE network interface 'uesimtun0' configuration highlighting the UE service initiation successfully.

References

1. Benzaïd, C.; Taleb, T.; Farooqi, M.Z. Trust in 5G and beyond networks. *IEEE Netw.* **2021**, *35*, 212–222. [CrossRef]
2. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Gurtov, A.; Ylianttila, M. Security for 5G and beyond. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3682–3722. [CrossRef]
3. Bica, I.; Unc, R.L.; Turcanu, S. Virtualization and Automation for Cybersecurity Training and Experimentation. In *Innovative Security Solutions for Information Technology and Communications; Proceedings of the 13th International Conference, SecITC 2020, Bucharest, Romania, 19–20 November 2020*; Revised Selected Papers 13; Springer: Cham, Switzerland, 2021; pp. 227–241.
4. Onoja, D.; Hitchens, M.; Shankaran, R. DDoS Threats and Solutions for 5G-Enabled IoT Networks. In *Secure and Trusted Cyber Physical Systems: Recent Approaches and Future Directions*; Springer: Cham, Switzerland, 2022; pp. 115–133.
5. Park, S.; You, I.; Park, H.; Kim, D. Analyzing RRC Replay Attack and Securing Base Station with Practical Method. In Proceedings of the 17th International Conference on Availability, Reliability and Security, Vienna, Austria, 23–26 August 2022; pp. 1–8.
6. Humayun, M.; Hamid, B.; Jhanjhi, N.; Suseendran, G.; Talib, M. 5G network security issues, challenges, opportunities and future directions: A survey. *J. Phys. Conf. Ser.* **2021**, *1979*, 012037. [CrossRef]
7. Park, S.; Kim, D.; Park, Y.; Cho, H.; Kim, D.; Kwon, S. 5G security threat assessment in real networks. *Sensors* **2021**, *21*, 5524. [CrossRef]
8. Salazar, Z.; Zaidi, F.; Mallouli, W.; Cavalli, A.R.; Nguyen, H.N.; de Oca, E.M. A formal approach for complex attacks generation based on mutation of 5G network traffic. In Proceedings of the International Conference on Software and Data Technologies, Lisbon, Portugal, 11–13 July 2022; Volume 1, pp. 234–241.
9. Nie, S.; Zhang, Y.; Wan, T.; Duan, H.; Li, S. Measuring the deployment of 5G security enhancement. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, San Antonio, TX, USA, 16–19 May 2022; pp. 169–174.
10. Salazar, Z.; Nguyen, H.N.; Mallouli, W.; Cavalli, A.R.; Montes de Oca, E. 5Greplay: A 5G network traffic fuzzer–application to attack injection. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; pp. 1–8.
11. Hussain, S.R.; Echeverria, M.; Karim, I.; Chowdhury, O.; Bertino, E. 5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 669–684.
12. Vakaruk, S.; Mozo, A.; Pastor, A.; López, D.R. A digital twin network for security training in 5G industrial environments. In Proceedings of the 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI), Beijing, China, 5 July–15 August 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 395–398.
13. Jae-hak, Y.; Ki-jong, K.; Ik-kyun, K.; Dae-seong, M. Intelligent Cyber Training Center Technology Trends. *Electron. Commun. Trend Anal.* **2022**, *37*, 36–45.
14. Rebecchi, F.; Pastor, A.; Mozo, A.; Lombardo, C.; Bruschi, R.; Aliferis, I.; Doriguzzi-Corin, R.; Gouvas, P.; Romero, A.A.; Angelogianni, A.; et al. A digital twin for the 5G era: The SPIDER cyber range. In Proceedings of the 2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Belfast, UK, 14–17 July 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 567–572.

15. Open5GS. A C-Language Implementation of 5G Core and EPC. Available online: https://open5gs.org/ (accessed on 1 November 2023).
16. UERANSIM. UE and RAN Simulator for 5G. Available online: https://github.com/aligungr/UERANSIM (accessed on 1 November 2023).
17. NICE Cyber Range Guide. Available online: https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf (accessed on 1 November 2023).
18. Nock, O.; Starkey, J.; Angelopoulos, C.M. Addressing the security gap in IoT: Towards an IoT cyber range. *Sensors* **2020**, *20*, 5439. [CrossRef] [PubMed]
19. Kavallieratos, G.; Katsikas, S.K.; Gkioulos, V. Towards a cyber-physical range. In Proceedings of the 5th on Cyber-Physical System Security Workshop, Auckland, New Zealand, 8 July 2019; pp. 25–34.
20. Hallaq, B.; Nicholson, A.; Smith, R.; Maglaras, L.; Janicke, H.; Jones, K. CYRAN: A hybrid cyber range for testing security on ICS/SCADA systems. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2018; pp. 622–637.
21. Rodrigo, M.S.; Rivera, D.; Moreno, J.I.; Álvarez-Campana, M.; López, D.R. Digital Twins for 5G Networks: A modeling and deployment methodology. *IEEE Access* **2023**, *11*, 38112–38126. [CrossRef]
22. Chouliaras, N.; Kittes, G.; Kantzavelou, I.; Maglaras, L.; Pantziou, G.; Ferrag, M.A. Cyber ranges and testbeds for education, training, and research. *Appl. Sci.* **2021**, *11*, 1809. [CrossRef]
23. Karagiannis, S.; Magkos, E. Adapting CTF challenges into virtual cybersecurity learning environments. *Inf. Comput. Secur.* **2020**, *29*, 105–132. [CrossRef]
24. Chouliaras, N.; Kantzavelou, I.; Maglaras, L.; Pantziou, G.; Ferrag, M.A. A novel autonomous container-based platform for cybersecurity training and research. *PeerJ Comput. Sci.* **2023**, *9*, e1574. [CrossRef] [PubMed]
25. Amponis, G.; Radoglou–Grammatikis, P.; Lagkas, T.; Mallouli, W.; Cavalli, A.; Klonidis, D.; Markakis, E.; Sarigiannidis, P. Threatening the 5G core via PFCP DoS attacks: The case of blocking UAV communications. *EURASIP J. Wirel. Commun. Netw.* **2022**, *2022*, 124. [CrossRef]
26. Amponis, G.; Radoglou–Grammatikis, P.; Lagkas, T.; Ouzounidis, S.; Zevgara, M.; Moscholios, I.; Goudos, S.; Sarigiannidis, P. Generating full-stack 5G security datasets: IP-layer and core network persistent PDU session attacks. *AEU Int. J. Electron. Commun.* **2023**, *171*, 154913. [CrossRef]
27. Shorov, A. 5G testbed development for network slicing evaluation. In Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Saint Petersburg and Moscow, Russia, 28–31 January 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 39–44.
28. Rupprecht, D.; Jansen, K.; Pöpper, C. Putting {LTE} security functions to the test: A framework to evaluate implementation correctness. In Proceedings of the 10th USENIX Workshop on Offensive Technologies (WOOT 16), Austin, TX, USA, 8–9 August 2016.
29. OpenAirInterface. Available online: http://www.openairinterface.org/ (accessed on 1 November 2023).
30. OAI Simulator. Available online: https://gitlab.eurecom.fr/oai/openairinterface5g/wikis/OpenAirLTEEmulation (accessed on 1 November 2023).
31. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. Overview of 5G security challenges and solutions. *IEEE Commun. Stand. Mag.* **2018**, *2*, 36–43. [CrossRef]
32. Holtrup, G.; Lacube, W.; David, D.P.; Mermoud, A.; Bovet, G.; Lenders, V. 5G system security analysis. *arXiv* **2021**, arXiv:2108.08700.
33. Neto, F.J.D.S.; Amatucci, E.; Nassif, N.A.; Farias, P.A.M. Analysis for comparison of framework for 5G core implementation. In Proceedings of the 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 3–5 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5.
34. Free5GC: Open Source 5G Core Network. Available online: https://www.free5gc.org/ (accessed on 1 November 2023).
35. Park, C.; Bae, S.; Oh, B.; Lee, J.; Lee, E.; Yun, I.; Kim, Y. {DoLTEst}: In-depth Downlink Negative Testing Framework for {LTE} Devices. In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), Boston, MA, USA, 10–12 August 2022; pp. 1325–1342.
36. Chlosta, M.; Rupprecht, D.; Holz, T.; Pöpper, C. LTE security disabled: Misconfiguration in commercial networks. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, FL, USA, 15–17 May 2019; pp. 261–266.
37. Chlosta, M.; Rupprecht, D.; Holz, T. On the challenges of automata reconstruction in lte networks. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi, United Arab Emirates, 28 June–2 July 2021; pp. 164–174.
38. Kim, H.; Lee, J.; Lee, E.; Kim, Y. Touching the untouchables: Dynamic security analysis of the LTE control plane. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–22 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1153–1168.
39. Nahum, C.V.; Pinto, L.D.N.M.; Tavares, V.B.; Batista, P.; Lins, S.; Linder, N.; Klautau, A. Testbed for 5G connected artificial intelligence on virtualized networks. *IEEE Access* **2020**, *8*, 223202–223213. [CrossRef]
40. Salazar, Z.; Zaidi, F.; Nguyen, H.N.; Mallouli, W.; Cavalli, A.R.; De Oca, E.M. A Network Traffic Mutation based Ontology, and its application to 5G networks. *IEEE Access* **2023**, *11*, 43925–43944. [CrossRef]
41. Yadav, R.; Sousa, E.; Callou, G. Performance comparison between virtual machines and docker containers. *IEEE Lat. Am. Trans.* **2018**, *16*, 2282–2288. [CrossRef]

42. Lingayat, A.; Badre, R.R.; Gupta, A.K. Performance evaluation for deploying docker containers on baremetal and virtual machine. In Proceedings of the 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 15–16 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1019–1023.
43. Paskauskas, R.A. ENISA: 5G design and architecture of global mobile networks; threats, risks, vulnerabilities; cybersecurity considerations. *Open Res. Eur.* **2022**, *2*, 125. [CrossRef] [PubMed]
44. ETSI TS 133 512. 2020. Available online: https://www.etsi.org/deliver/etsi_ts/133500_133599/133512/16.03.00_60/ts_133512v160300p.pdf (accessed on 1 November 2023).
45. Wireshark. Available online: https://www.wireshark.org/ (accessed on 1 November 2023).
46. tcpdump. Available online: https://www.tcpdump.org/ (accessed on 1 November 2023).
47. Lee, R.B. *Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures*; Princeton University: Princeton, NJ, USA, 2004.
48. Vargas, P.; Tien, I. Impacts of 5G on Cyber-Physical Risks for Interdependent Connected Smart Critical Infrastructure Systems. *Int. J. Crit. Infrastruct. Prot.* **2023**, *42*, 100617. [CrossRef]
49. Lehr, W.; Queder, F.; Haucap, J. 5G: A new future for Mobile Network Operators, or not? *Telecommun. Policy* **2021**, *45*, 102086. [CrossRef]
50. Ahanger, T.A.; Aljumah, A.; Atiquzzaman, M. State-of-the-art survey of artificial intelligent techniques for IoT security. *Comput. Netw.* **2022**, *206*, 108771. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.