5G-Muffler: Covert DoS Attacks over Open Frounthaul Interface of O-RAN 5G Network

***Abstract*—Open Radio Access Network (RAN) movement promotes an open RAN vendor ecosystem by defining open RAN architecture and interfaces. The open fronthaul (O-FH) interface is a crucial interface between the O-RAN Radio Unit (O-RU) and the O-RAN Distributed Unit (O-DU), allowing mobile network operators to select best-of-breed O-RUs among multiple vendors. However, O-FH also introduces new security risk. In this work, we present *5G-Muffler*, a set of covert DoS attacks over the O-FH interface. 5G-Muffler disrupts the random access process, the initial step for a user equipment (UE) to connect to the network. By preventing UEs from completing this step, 5G-Muffler makes the 5G network inaccessible. Furthermore, the attack is invisible to anomaly detection mechanisms above PHY layer. Our first variant, 5G-Muffler-1, introduces a man-in-the-middle device between O-RU and O-DU by manipulating an O-FH switch's configurations. The second variant, 5G-Muffler-2, targets the common 5G shared-cell setup, where a cell uses multiple O-RUs to enhance its coverage and signal quality. 5G-Muffler-2 only needs to control a single O-RU and it leverages weakness in the shared-cell signal aggregation process to amplify the attack to the whole cell. We demonstrate 5G-Muffler on commercial O-RAN systems and propose countermeasures to mitigate these attacks.**

***Index Terms*—5G, Open RAN, O-RAN, Open Frounthaul interface, DoS, Random access, O-RU, O-DU**

I. Introduction

Open Radio Access Network (RAN) [1] movement aims to transform global telco ecosystem by promoting RAN disaggregation, open and interoperable interfaces, RAN virtualization, and AI-enabled RAN intelligence. The O-RAN ALLIANCE, founded by mobile network operators (MNOs) around the world, specifies the open RAN architecture and various O-RAN interfaces, which lays the foundation to foster interoperability among disaggregated cellular network equipment from diverse vendors [2]. In particular, the O-RAN ALLIANCE has specified the open frounthaul (O-FH) interface, which defines the interaction between an O-RAN Radio Unit (O-RU) and an O-RAN Distributed Unit (O-DU) through the utilization of the 3GPP 7.2x functional split. This split divides the physical layer (PHY) into PHY-high and PHY-low components. O-FH allows O-RUs from different vendors to be used in an MNO's network, giving MNOs the power to mix and match best-of-breed solutions without being locked-in by specific vendors. The O-FH includes four planes, which are the control plane (C-Plane), the user plane (U-Plane), the management plane (M-Plane), and the synchronization plane (S-Plane) to exchange messages between the O-RU and the O-DU [3], [4]. The transport protocol of O-FH is eCPRI (Enhanced Common Public Radio Interface). eCPRI has significantly improved data transmission efficiency and scalability between O-RU and O-DU. Together with O-FH's important role in disaggregating the RAN also comes new security risk. In particular, there are more open components in the frounthaul of a 5G network, such as O-RUs from different vendors and O-FH switches that connect O-RUs and O-DUs. These new open components are subject to various forms of attacks and expand the attack surface of a 5G system. Furthermore, due to strict performance requirements and the lack of maturity in some O-RAN vendors' technology, there are a lack of security features in the frounthaul network.

In this work, we introduced *5G-Muffler*, a set of covert Denial-of-Service (DoS) attacks over the open fronthaul interface of O-RAN 5G networks. The aim of 5G-Muffler is to make the targeted 5G networks inaccessible to user equipment (UE). A key consideration for the design of 5G-Muffler attacks is to make them invisible to any security defence mechanism above the PHY layer. As such, we target the random access process, which is the initial step for a UE to connect to 5G systems. In particular, our proposed attack targets the first message sent from the UE to the network (referred to as Msg1), which contains a random access preamble selected by the UE from a set of preambles predefined by the network. If network cannot decode Msg1 correctly, no follow-up communications will happen. Hence, it is a critical choking point for the whole 5G network. Attacking Msg1 is also easier than attacking messages after the Authentication and Key Agreement (AKA) procedure, where a security context for encryption and integrity protection is set up. This is because by design, Msg1 is not encrypted, nor integrity-protected. Therefore, an attacker can manipulate the message without the need to have access to any security keys between UE and network. We carry out the 5G-Muffler attack over the O-FH. We find that in several commercial-grade O-RAN 5G systems, there is no integrity protection or replay attack prevention mechanisms for the IQ samples carried by eCPRI packets in their O-FH implementation. Such a lack of protection at the O-FH makes our proposed attacks easier to carry out. Last but not the least, as the proposed attacks target the processing at the PHY layer, i.e., the preamble detection in the random access process, it is perfectly invisible to any anomaly detection mechanisms at higher layers. When 5G-Mufller succeeds, the O-DU does not correctly detect the random access preamble sent by UEs, hence the network will not respond to the UEs in the expected manner.

We propose two variants of the 5G-Muffler attack in this paper. The first, *5G-Muffler-1*, involves the sophisticated ma-

nipulation of features in an O-FH Ethernet switch to establish a man-in-the-middle (MitM) node between the O-RU and O-DU. Once the MitM node is set up, it can intercept and alter communications transparently. The second variant, *5G-Muffler-2*, targets the widely used 5G shared-cell setup, where a cell utilizes multiple O-RUs to enhance coverage and signal quality. By controlling a single O-RU, *5G-Muffler-2* can use the weakness in the shared-cell signal aggregation process to amplify the impact of its attack to the whole cell, ultimately blocking any UE in the targeted cell from connecting to the 5G network, even if other non-compromised O-RUs correctly forward the UE's preamble to the O-DU and even if the compromised O-RU cannot communicate with the targeted UE at all. In summary, the main contributions of this paper are:

- We present 5G-Muffler, a set of covert DoS attacks on open fronthaul interface. To be stealthy, 5G-Muffler targets the random access procedure, which is the first step for an UE to connect to a network. We describe two variants of 5G-Muffler under two different threat models.
  - In 5G-Muffler-1, we assume the attacker can manipulate the O-FH switch settings and have access to a device attached to the switch that serves as the MitM node. Under this setting, we show that it is both practical and stealthy to launch a MitM attack method to silently block Msg1.
  - In 5G-Muffler-2, we assume the attacker can manipulate one O-RU, which is part of a cell that contains multiple O-RUs. 5G-Muffler-2 exploits the weakness in the shared-cell signal aggregation process to DoS all the UEs that want to connect to the cell.
- We demonstrated the effectiveness of both variants of 5G-Muffler attacks using a commercial O-RAN system. Specifically, we show that the attacks prevent UEs from registering with the 5G system and do not leave trace above the PHY layer stack in O-DU, nor over the air.
- We proposed several approaches to counter 5G-Muffler attacks. We recommend such measures be considered in O-RAN best practice to mitigate the risk of such covert DoS attacks.

The paper is structured as follows. Section II examines existing attack techniques to 5G networks and the implications of O-RAN to 5G security. Section III outlines the threat model and the underlying system assumptions. Section IV provides background information about open fronthaul, 5G initial access, and shared cell. The details of the 5G-Muffler attacks are presented in Section V. We present the evaluation results and discuss potential counter measures in Section VI. The paper is concluded in Section VII with future work.

II. RELATED WORK

Numerous studies have been conducted on the security of cellular networks. O-RAN-based systems have been considered in some of these studies (e.g., [5]) or used in prototyping some of the attacks (e.g., [6]).

One common type of attack involves setting up fake base stations [7], where attackers lure victim UEs to connect to fake base stations by transmitting a stronger signal than the legitimate cell. For example, the authors of [8] introduce a novel physical signal overshadowing attack (SigOver) on LTE systems. This attack manipulates the timing and frequency of the broadcast signal slightly to overshadow legitimate signals, causing UEs to decode only the attacker's signal. While the SigOver attack demonstrates potential threats to LTE systems by exploiting vulnerabilities in broadcast signaling and SigOver significantly reduces the transmission power required by the attacker as compared to the legitimate transmission power, it still requires the attacker to be at the proximity of the targeted UEs and emit signal to the air. Hence, if the attacker wants to attack a large area or affect UEs that are far away, the emitted signal can be used for detection. For example, in the 5G security specification 3GPP TS 33.501 [9], a device-assisted network-based detection is specified, where the network can configure UEs to scan selected radio frequencies periodically and report the collected statistics (such as received-signal strengths). The network then can analyze the reported information and cross check with relevant information such as network cell topology to detect anomaly. When the analysis shows potential indicators of false base stations, more detailed scanning can be carried out in the identified region, e.g., by law enforcement.

Another type of attack involves using the malicious UEs [10] to carry out attacks. Such attacks usually explore some weakness in the 5G or 4G/LTE protocol design or implementation. For example, the recent 5G-SPECTOR work [6] looks into security problems in Layer-3 (L3) cellular protocols in 5G networks. They developed a framework to detect known attacks in cellular networks based on an O-RAN architecture. Their study mainly focuses on implementing and identifying existing 4G/5G attacks and does not not focus on new attacks that are made possible by the open RAN design. Our research, on the other hand, focuses on how to use weaknesses in the open fronthaul (O-FH) interface to perform covert DoS attacks that stop devices from connecting to the network. The 5GReasoner framework [11] highlights several cutoff attacks on 5G control-plane protocols, which often require knowledge of the TMSI and can be detected by the 5G core if discrepancies arise from subsequent legitimate UE messages. In contrast, our 5G-Muffler attacks target the Physical Random Access Channel (PRACH) and do not need such prior knowledge. By focusing on the random access process, our attacks remain undetectable by higher-layer anomaly detection systems and do not rely on subsequent UE behavior, which could expose traditional cutoff attacks. This makes 5G-Muffler a more straightforward and stealthier method for rendering the 5G network inaccessible.

Specific to O-FH interface which is defined by O-RAN ALLIANCE working group 4 [12], its threat model and security analysis is conduced in [13]. Security test cases related to O-FH is defined in [14] and recommended security measures are defined in [14], [15]. While these specifications cover several basic aspects of O-FH security, they do not enumerate new forms of attacks that can exploit the unique properties in O-FH. Even for attacks and countermeasures

defined in these O-RAN specifications, they have not been widely supported by the O-RAN vendors. For example, the work [5] implements the C-plane Denial of Service (DoS) attack on the O-FH based on [14]. They test a couple of commercial O-RAN solutions under such standard volume-based DoS attacks. They utilized the source code offered by the O-RAN Software Community (OSC) to create a software tool for generating C-Plane DoS attack packets. By adjusting the MAC address and injecting these spoofed packets into the testbed, they assessed the robustness of O-RAN systems under such attacks. However, such attacks generate significant additional traffic at O-FH. They cause degradation of the UE's performance (such as throughput, and end-to-end delay), hence, they can be detected by higher-layer anomaly detection mechanisms that monitor the network and UE performance.

In the work [16], the author highlights a MitM attack involving the introduction of random packet delays on Precision Timing Protocol (PTP) sync messages and/or PTP delay-request/response messages. This interference leads to inaccurate PTP offset calculations, potentially causing clocks to be improperly synchronized, thus resulting in a Denial of Service (DoS) attack. The RAN typically cannot be established successfully if PTP fails. Hence, such attack can be easily detected by today's cellular network monitoring solutions.

III. THREAT MODEL

We consider two threat models that cover major attack vectors to an O-FH network. The targeted O-FH network can be part of an MNO network or an enterprise network dedicated to specific use cases, e.g., smart factories, air/sea ports, or supporting big events. We consider stealthy attackers who aim to make such networks unavailable to intended users. Their objectives are to disrupt the services in short term and undermine the reputations of the targeted MNO or O-RAN vendors in long term.

In the first threat model, we assume an attacker can access the O-FH switch through a device directly connected to the switch. One such device can be an engineering station or monitoring device attached to the O-FH network. The attacker can either be a malicious insider or she can obtain such access through social engineering. We assume the compromised device has high-speed connection to the O-FH switch and can execute malicious code. These two requirements are needed to alter O-FH packets on line speed. We assume the attacker manages to gain administrative privileges on the O-FH switch — this could be achieved easily if the switch uses weak or default password, or if the compromised engineering device has been granted such access. Otherwise, the attacker needs to gain such access through social engineering or privilege escalation. Given the openness of O-RAN vendor ecosystem, it is also possible that the attackers gain all required privileges to the O-FH network through systematic supply chain attack.

Under this first threat model, we also exploit the lack of integrity protection mechanisms at eCPRI or at the layers below when eCPRI carries O-FH's C/U/S/M plane traffic. Many commercial-grade O-RAN solutions today only uses application layer integrity protection for the M-Plane. This leaves the C/U/S planes vulnerable to Layer-2 security threats [4]. Once an adversary gains Layer-2 access as in our threat model, they can insert/replay eCPRI messages or alter specific fields in legitimate packets. Our paper primarily concentrates on manipulating the U-plane packets that carry the IQ samples.

Our second threat model involves an attacker compromising an O-RU to alter its packet processing logic. Again, the attacker may be an insider or she can use social engineering to obtain administrative privileges to upload malicious firmware to the targeted O-RU. This malware then modifies the internal packet processing logic in the O-RU. While we assume the attacker can already make arbitrary change to the compromised O-RU, the attacker's goal is to do more harm than what can be achieved at the compromised O-RU alone. We think this threat model is especially relevant for an O-RAN system, where O-RU from different vendors are combined to provide different ranges of coverage (e.g., a massive MIMO O-RU from one vendor to provide outdoor coverage, together with a 4T4R O-RU from another vendor to provide indoor coverage). Given such diversity of vendors, the risk of having one compromised O-RU could be higher than the traditional single-vendor system. We will show how the attacker can amplify its attack impact beyond the single O-RU it controls to affect regions covered by other non-compromised O-RUs when they are jointy used to support the shared-cell setup.

IV. BACKGROUND

A. Open-RAN Fronthaul

Open RAN represents a paradigm shift from traditional radio access networks (RANs), which are characterized by closed, vertically integrated solutions where a single vendor provides both hardware and software, leading to vendor lock-in and limited innovation. Open RAN disaggregates network elements, enabling operators to choose the best solutions from different vendors.

The O-RAN ALLIANCE, established in 2018, plays a pivotal role in promoting an open RAN architecture built on 3GPP standards with additional interfaces and functions [12]. In the 3GPP-based architecture [17], the gNB is divided into the Centralized Unit (CU) and the Distributed Unit (DU), known as the High Layer Split (HLS). In O-RAN, the DU is further divided into the Open-Distributed Unit (O-DU) and the Open-Radio Unit (O-RU), referred to as the Lower Layer Split (LLS), as shown in Fig. 1. The O-CU, serving as the central control and management unit, implements protocol layers such as SDAP, PDCP, and RRC, with the user plane (UP) and control plane (CP) split into CU-UP and CU-CP submodules. The O-CU works closely with the O-DU to manage data flow and radio bearers effectively, ensuring flexibility and interoperability among different vendors. The O-DU handles distributed processing of data and radio functions, implementing the high PHY and Layer 2 (L2) layers of the New Radio (NR) protocol stack, including NR MAC, NR Scheduler, and NR RLC.

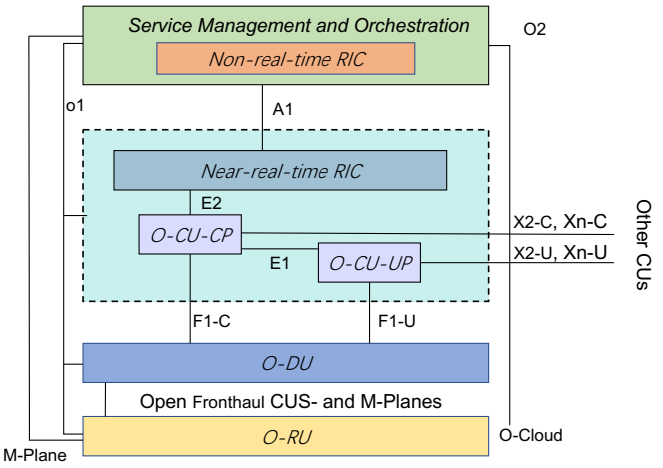

Fig. 1. O-RAN architecture

eCPRI Common Header					eCPRI Payload
eCPRI Protocol Revision	Reserved	C	eCPRI Message Type	eCPRI Payload Size	
4 Bit	3 Bit	1 Bit	8 Bit = 1 Byte	16 Bit = 2 Bytes	0 - 65535 Bytes

Fig. 2. eCPRI packet format

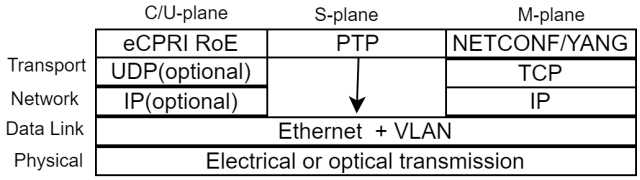

Fig. 3. S/M/C/U planes between O-RU and O-DU

Fig. 4. 5G Initial Access (RACH) process

The O-FH interface, crucial for multi-vendor interoperability in Open RAN, connects the O-DU and O-RU, facilitating their communication and coordination. Defined by the O-RAN ALLIANCE Work Group 4 based on RAN function split 7-x and the eCPRI standard, this interface supports the transport of data across four planes, as depicted in Fig. 3:

- Control Plane (C-Plane): Provide instantaneous control information to the O-RU via eCPRI to specify the handling of User Plane traffic.
- User Plane (U-Plane): Transfer real-time uplink and downlink IQ data samples through eCPRI for the traffic transmitted over the air.
- Synchronization Plane (S-Plane): Send periodic timing and synchronization messages using the IEEE 1588 Precision Time Protocol (PTP) to synchronize the O-RU with the network.
- Management Plane (M-Plane): Provide non-real-time management based on NETCONF/YANG models.

The encapsulation of C/U/S/M-Planes packets is illustrated in Fig. 3. The S-Planes are directly encapsulated over Ethernet, whereas the M-Plane utilizes TCP and IP for transport. Depending on the specific use case, CU planes may be transported over UDP, IP, and Ethernet. Due to performance consideration, many O-RU implementations encapsulate CU plane traffic directly over Ethernet without any integrity protection, making them susceptible to Layer 2 threats [18].

B. eCPRI

eCPRI (enhanced Common Public Radio Interface) is used in O-FH network, addressing the need for higher bandwidth, lower latency, and flexible deployments [19]. By connecting O-RU and O-DU with optimized transport of radio signals over Ethernet, eCPRI enables a scalable RAN architecture.

The eCPRI packet structure includes a common header and a payload. The common header consists of fields such as eCPRI Protocol Revision, Concatenation Indicator to indicate if multiple eCPRI messages are concatenated, eCPRI Message Type identifying the type of eCPRI message, and eCPRI Payload Size specifying the size of the payload in bytes, as shown in Fig. 2. The payload for U-plane typically contains the IQ data, representing the in-phase and quadrature components of the signal, which are crucial for modulating and demodulating the radio signal.

As eCPRI technology gains traction, its security concerns have garnered attention [20], [21]. The primary security challenges stem from its open and decentralized architecture, which, while enhancing flexibility and scalability, also introduces potential entry points for unauthorized access and data breaches.

C. 5G Initial Access

The 5G Random Access Channel (RACH) is essential for UEs to initiate connections to the 5G network [22]. Fig. 4 shows the procedure [23].

- The base station periodically broadcasts a Synchronization Signal Block (SSB) across all beams at various intervals, called an SSB burst. This SSB contains essential information, including timing for the UE to transmit the RACH signal. It also sends the System Information Block 1 (SIB1), which includes RACH configuration details to determine the preamble format.

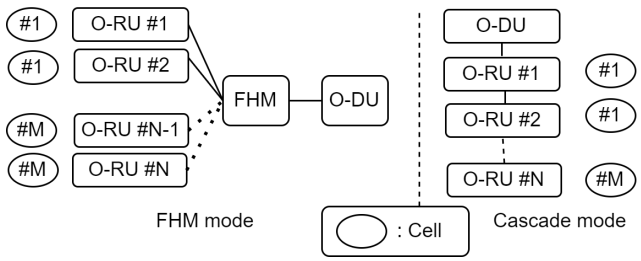

Fig. 5. Shared-cell

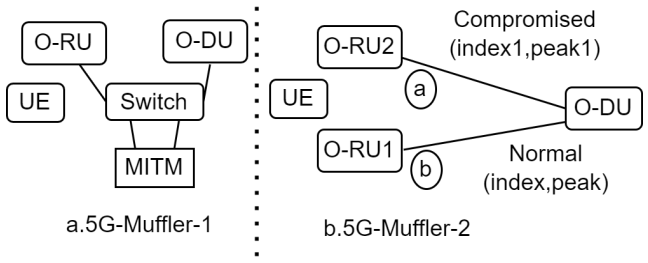

Fig. 6. Setup for the 5G-MUFFLER-1 and 5G-MUFFLER-2

- Msg1 (Preamble Transmission): The UE measures the SSBs on all beams, selects the one with the strongest signal, and decodes it to determine the RACH reception window. During this window, the UE randomly chooses one of the 64 preambles and transmits it on the Physical Random Access Channel (PRACH).
- Msg2 (Random Access Response): The network detects the received preamble and replies with critical information, such as the Time Advance (TA) command for timing adjustment, the Random Access Preamble ID (RAPID) corresponding to the preamble transmitted by the UE, and an initial uplink grant. The 5G base station also assigns a Random Access Radio Network Temporary Identifier (RA-RNTI) to the UE. Upon receiving the RAR, the UE validates the RAPID value with the preamble index sent in Msg1. If they match, the UE proceeds to send Msg3; if not, the UE will retry.
- Msg3: The UE will send Message 3 over the Physical Uplink Shared Channel (PUSCH). Msg3 may contain a specific RRC message (e.g, RRCRequest).
- Msg4 (Contention Resolution): Incorporating the UE's identity, this message serves as a confirmation that the 5G base station has recognized the UE, and any contention has been successfully resolved.

D. Shared Cell

A shared cell setup is a widely adopted practice when deploying cellular systems. It allows the use of multiple radio units to operate together and form the same cell coverage for UEs [12]. By using multiple O-RUs, the cell enhance its coverage and signal quality. It can be configured and operated in two modes which are Fronthaul Multiplexer (FHM) mode and Cascade mode as shown in Fig. 5. For FHM mode, the FHM copies the downlink IQ samples and send to all O-RUs, and it combines the uplink signals from all O-RUs through a signal aggregation process. While for cascade mode, it is realized by several O-RUs cascaded in a chain. The O-RUs in the cascaded chain except for the last O-RU shall support Copy and Combine function. Our second threat model is applicable to both modes and the compromised O-RU can be any O-RU that forms the shared cell.

V. 5G-MUFFLER

We now introduce the two main variants of our proposed covert 5G DoS attack over O-FH interface, corresponding to the two threat models presented in Section III.

A. 5G-Muffler-1

The fronthaul latency restrictions between the O-DU and O-RU are stringent, with an even more stringent synchronization time error requirement. 5G-Muffler-1 is designed to meet these performance standards. It is particularly suitable for configuration that includes one fronthaul switch connecting one O-RU and one O-DU, as illustrated in Fig 6.a.

1) MITM design: To attack this configuration, an attacker would need to control that switch and a PC with two network ports that connect to this same Ethernet switch, and gain control of the switch. There are S/M/C/U packets passing through the switch between the RU and DU, which demand very high throughput. Common MITM packet crafting technologies, such as nfqueue and Scapy, cannot meet these requirements. Therefore, we developed an application based on Data Plane Development Kit (DPDK) to handle the packet modification tasks. We also utilized the switch's Static MAC table and VLAN translation mapping table to redirect the C/U plane packets to our application while keeping the S/M plane flow direction unchanged. This is due to the more stringent synchronization time requirement of PTP. With this method we can ensure the PTP get synchronized and the application is fast enough to handle the eCPRI throughput as well.

2) Preamble generation, transmission and detection: Once the MITM setup is successful, the attackers can identify the received preambles and craft fake preambles to confuse the 5G preamble detection system.

Zadoff-Chu (ZC) sequence The preamble sequence is generated based on ZC sequences, it is a construction of Frank-Zadoff sequences defined by D. C. Chu [24]. They have special properties that make them ideal for the PRACH process

- Constant Amplitude: This sequence has a consistent magnitude, which benefits communication systems by maintaining stable power levels and simplifying implementation. The sequence, consisting of real and imaginary components, forms a complex number. On a complex plane (constellation), all points lie in a circle.
- Cyclic Shift: It exhibits cyclic shift-orthogonality, meaning the correlation between a ZC sequence and its cyclically shifted versions is zero. The preamble index can be represented by different cyclic shifts.
- Good Auto-Correlation: It shows zero correlation with its cyclically shifted versions except for a distinct peak at the

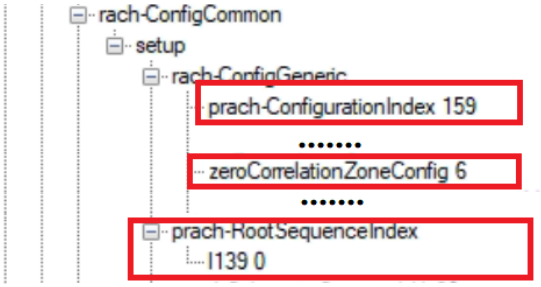

Fig. 7. Parameters in SIB1

shift. This makes it ideal for the preamble process, as the peak enables differentiation between sequences.

- Low Cross-Correlation: To generate 64 preambles, multiple root sequences are needed, this is to ensure low cross-correlation between different root sequences.

Preamble generation When a UE successfully receives and decodes the SIB1 from a 5G system, its primary goals are to determine the type of preamble it needs to send and the timing for sending the preamble.

There are many parameters in SIB1 as shown in Fig. 7 related to RACH configuration. But these three parameters are related to the preamble generation which is $prachConfigIndex$, $prachRootSequenceindex$ and $zeroCorrelationZoneConfig$. Fig. 8 shows the steps.

- ①: 5G supports two sequence lengths: long and short preambles. Long preambles, with a length of 839, come in four formats from LTE and have subcarrier spacings of 1.25 kHz and 5 kHz, usable frequency range (FR1) is below 6 GHz. Short preambles, with a length of 139, are defined in eight new formats (A1, A2, B1, B2, B3, B4, C1, C3). These do not support high-speed UEs and can be used in both FR1 and FR2 (frequency range is above 6 GHz). The UE extracts the $prachConfigIndex$ from SIB1 and determines the correct preamble format by referring to Configuration Mapping Table 1, based on the UE operating frequency range.
- ②: The UE needs to search Configuration Mapping Table 2 to find the correct table for mapping from $prachRootSequenceIndex$ to the sequence number u.
- ③: $ZeroCorrelationZoneConfig$ determine the cyclic shift(Ncs) value.
- ④: Nzc is 839 for the long format and 139 for the short format.The based base sequence can be obtained by inputting Nzc and u.
- ⑤:with the base sequence and Ncs and UE can generate the 64 preambles

Preamble transmission The preamble is only permitted to be transmitted at specific occasions. An occasion refers to a designated interval within the time and frequency domains set aside for receiving preambles. UEs are allowed to send preambles exclusively during this period. As illustrated in step ① of Fig. 8, the $prachConfigIndex$ determines the details of these occasions, including the subframe number, start symbol number, and sequence duration.

Preamble detection A 5G system must include a preamble detector to identify multiple access requests. This detector should distinguish between noise alone and preamble requests amidst noise and interference. By computing the cross-correlation function between the received PRACH preamble sequence and a root ZC sequence, a threshold value is established. This threshold determines whether access requests are present and affects the probabilities of false alarms and detection. The implementation of the preamble detector may vary by vendor based on their specifications.

B. 5G-Muffler-2

5G-Muffler-2 targets the widely used 5G shared-cell setup, where signals from multiple O-RUs are aggregated. By exploiting weaknesses in the aggregation process, we can control just one RU and amplify the attack to affect other RUs

1) Attack design: Fig. 6.b illustrates the design, where O-RU2 has been compromised by an attacker, resulting in the output preambles from O-RU2 also being compromised. Consequently, the 5G system will receive both normal and compromised preambles simultaneously. Our focus will be on the behavior of the 5G system.

2) Signal aggregation: In the downlink scenario, eCPRI messages originating from the O-DU are copied and forwarded to each O-RU without modification. Conversely, in the uplink scenario, IQ data from the same radio resource element should be combined and sent to higher layers. For example, Fig. 9 illustrates how the IQ data is combined for the uplink direction.

3) Correlation peak: The correlation peak is crucial for the 5G system to determine the preamble index. By analyzing the eCPRI's IQ data, we can manually identify the preamble index using Matlab code. The eCPRI's IQ data represents the received signal in the frequency domain. It is multiplied by the complex-conjugate frequency-domain representation of the root ZC sequence and fed through an IFFT. The IFFT output reveals the transmitted shift of the root ZC sequence and its delay, with a peak indicating the cyclically shifted sequence.

In Fig. 10, a ZC sequence with rootSequenceIndex 0 and cyclic shift Ncs of 12 shows that preamble 1 will be at offset 12, and preamble 2 at offset 24. The sharp correlation peaks at positions 13 and 25, occurring just after the cyclic shift, confirm the preamble detection, with all other positions showing zero correlation and a peak value of 139.

VI. Evaluation and Countermeasures

Several experiments were conducted on a commercial 5G system to validate the effectiveness of 5G-Muffler.

A. Case study: A commercial 5G system

We use a real commercial 5G system that follows Intel FlexRAN implementation. It is necessary to treat this system as a black box, as there is no information available to us regarding the eCPRI. We first sniff the eCPRI traffic and find the following properties:

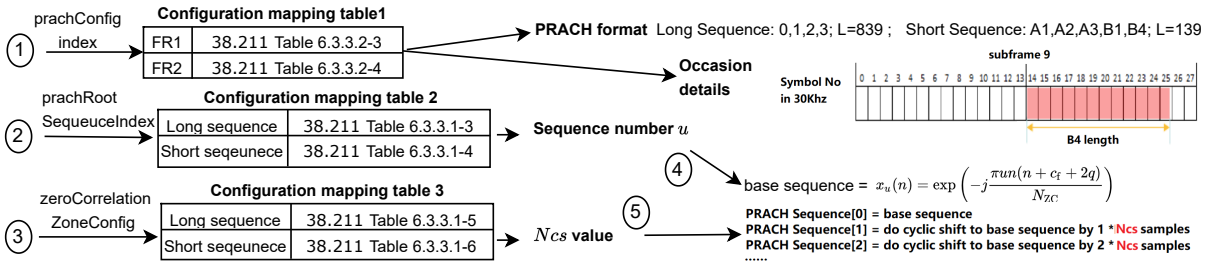

Fig. 8. Preamble generation

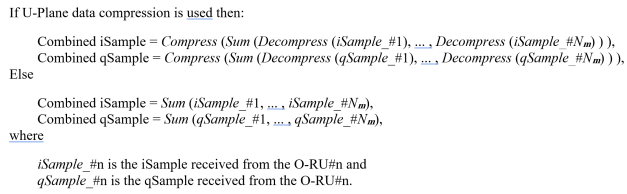

Fig. 9. Uplink combination under FHM mode

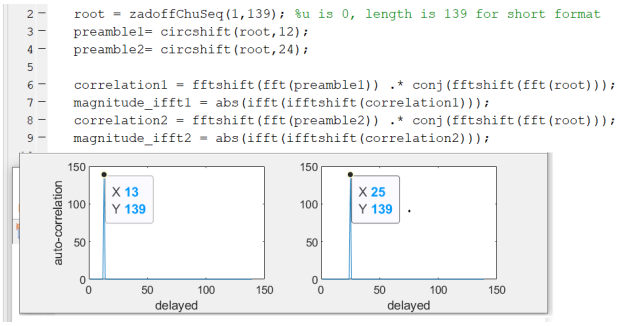

Fig. 10. Preamble detection

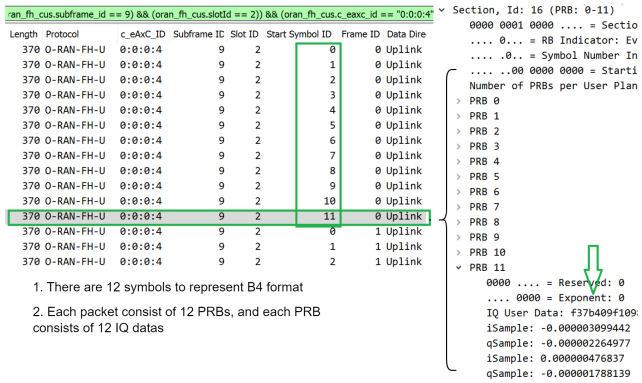

Fig. 11. eCPRI packets for preambles

- **Configuration parameters** As shown in Fig. 7, The $prachConfigurationIndex$ is 159, $zeroCorrelationZoneConfig$ is 6 and $preachRootSequeneceIndex$ is 0. Therefore we can tell the preamble's format is short format B4 which consists of 12 sequences as shown in Fig. 8, the preambles are only allowed to be sent in subframe 9, 2nd slot which is symbol #14 when it is operated on 30Khz. And the duration is 12 symbols from symbol #14 to #25. By analyzing the eCPRI packets, we can find the mapping shown in Fig. 11. There are 12 packets for each frame, corresponding to subframe ID 9, slot ID 2, and start symbols 0 to 11. Each packet consists of 12 PRBs and each PRB contains 12 IQ data points.
- **Preamble identification** We can identify the packets that contain preambles by using the occasion, in this system, which is subframe 9, slot 2. and then we plot the constellation in Fig. 14, we can observe that in Fig. 14.a is the noise value and its magnitude is very low, while Fig. 14.b is the preamble that UE is located at a place that close to the RU, it has a good circle pattern. It becomes clear that it is the preamble once you observe the plot. But for Fig. 14.c, It will be difficult to determine if it is a preamble just by looking at the plot. Although it is still a preamble, it was captured when the UE and RU were far apart. We use a circular checking method to identify whether it is a preamble or not. The core concept involves examining the magnitude of each point and then ensuring the points follow a circular trajectory by evaluating the angles formed by any three consecutive points in each PRB. First, we analyze the initial three non-zero IQ points to determine whether the rotation is anticlockwise or clockwise. Then, we examine the remaining points. If most of their rotation directions match the initial direction, we can classify this PRB as a circular type. This process is repeated for all 12 PRBs to determine whether the packet is a preamble.
- **Signal aggregation** We are uncertain about its internal configuration. However, eCPRI packets captured from both O-RUs show that they receive eCPRI with the same targeted eAxC ID for the same occasion. This indicates some signal combination is occurring, though the exact mechanism is beyond the scope of this paper.

B. 5G-Muffler-1

1) MITM setup: Fig. 12 shows the detailed steps to redirect the O-FH traffic on the real commercial system by using the

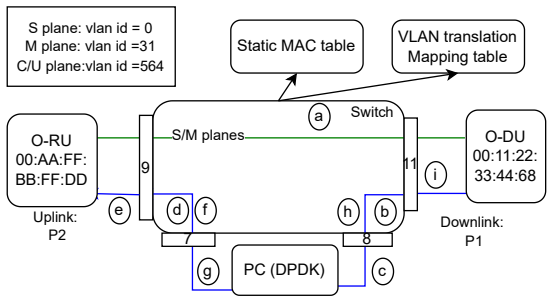

Fig. 12. MITM set up

a. Static MAC Table

	Delete	VLAN ID	MAC Address	Port Members 1	2	3	4	5	6	7	8	9	10	11
Rule 1	☐	563	00-11-22-33-44-68	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑
Rule 2	☐	564	00-AA-FF-BB-FF-DD	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐
Rule 3	☐	565	00-AA-FF-BB-FF-DD	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐

b. VLAN Translation Mapping Table

	Group ID	Direction	VID	TVID	
Rule 1	7	Egress	564	563	⊕⊗
Rule 2	8	Egress	564	565	⊕⊗
Rule 3	9	Egress	565	564	⊕⊗
Rule 4	11	Egress	563	564	⊕⊗

Fig. 13. Static MAC table and VLAN translating mapping table

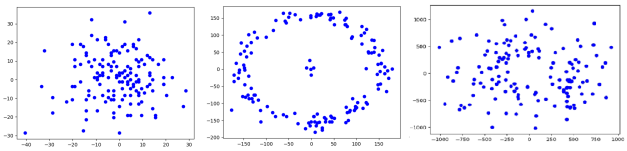

Fig. 14. The constellation diagram of noise packet vs Msg1 packet

switch's functions. The S/M/C/U has a different VLAN id. And We can use the static MAC table and VLAN translation mapping table to redirect the traffic.

Firstly, link ⓐ is the original link between O-RU and O-DU. Assume O-RU connects to the Port 9 of the switch, and O-DU connects to Port 11 of the same switch. And all S/M/C/U plane data through this established link. Secondly, segregate the S/M planes from C/U planes. Redirect C/U planes to the MITM device by configuring the Static MAC table and VLAN translation mapping table in Fig. 13 on the switch. It contains multiple steps shown below:

- Steps ⓑ, ⓒ, ⓓ, and ⓔ are involved in the downlink traffic. The first eCPRI downlink packet, P1, is sent from the O-DU to the O-RU. Step ⓑ, when P1 arrives at port 11, the switch will redirect it to port 8 by checking Rule 2 in Fig. 13.a. To prevent the switch's MAC learning, we need to change the vlan id. Step ⓒ ensures that port 8 changes the egress packet's vlan id from 564 to 565 according to Rule 2 in Fig. 13.b. Step ⓓ, when the P1 arrives at port 7, it will redirect to port 9 according to Rule 3 in Fig. 13.a. Finally, we need to change back the VLAN id from 565 to 564 in step ⓔ by checking Rule 3 in Fig. 13.b.
- Steps ⓕ, ⓖ, ⓗ, and ⓘ are involved in the uplink traffic. Once the O-RU receives P1, it replies to the O-DU with a uplink packet, P2. In step ⓕ, a mirror port is enabled to is mirror RX only packets on port 9 to port 7. In step ⓖ, the vlan id of packets egressing from port 7 is translated from 564 to 563 by configuring Rule 1 in Fig. 13.b. In step ⓗ, packet P2 is forwarded to port 11 by checking Rule 1 in Fig.13.a. In step ⓘ, the vlan id is changed back to 564 according to rule 4 in Fig. 13.b.

Finally, the MITM node is established as expected.

TABLE I
PREAMBLE ATTACKS

No	Attack steps	Description	Result
1	Change eCPRI type 0xaefe to 0xffff	This packet to be invalid	✗
2	Change IQ payload to 0	This packet still valid, but the IQ signal to be 0	✗
3	Change IQ payload to other preamble index	This packet still valid, but modify with different preamble index	✗
4	Change IQ payload to the noise type in Fig 14.a	This packet still valid, but the IQ payload is noise	✗

2) Preamble attacks: With the setup, we can carry out different attacks. Table I shows the 4 scenarios, the purpose is to obstruct Msg1, leading to the anticipated outcome of the UE failing to register and also ensuring the attack is covert and inconspicuous. In scenario #1, modifying the eCPRI type from 0xaefe to 0xffff renders the packet invalid for eCPRI, preventing its use by the 5G system. As a result, this procedure is akin to discarding Msg1. The current attack is too conspicuous to go unnoticed; hence, some modifications are necessary. In scenario #2, we ensure the packet remains a valid eCPRI packet, but with a zero IQ signal. Consequently, we observe the UE's failure to register, However, in a real-life environment, it is very uncommon to receive zero IQ payload packets due to the presence of noise. In scenario #3, by creating a fake Msg1 with a different preamble index. The UE will receive an RAR with a different RAPID which causes the validation process to fail. Identifying the issue can be quite challenging if you are debugging only on one side. For all the above scenarios, we can apply the occasion plus the circular checking method to identify the actual preambles. In scenario #4, we just modify all the packets filtered by occasion condition to be noise pattern shown in Fig. 14.a, the modified packet appears identical to a typical noise packet. This adjustment enhances the attack's covert and inconspicuous nature. Consequently, the UE registration is unsuccessful.

C. 5G-Muffler-2

1) Experiment 1: From the results of the 5G-Muffler-1 experiment, all test cases listed in Table I effectively prevented the UE from registering. However, when the same experiments

TABLE II
ATTACKS ON ONE RU'S PREAMBLE CORRELATION PEAK

Exponent value	1	2	3	4	5	6	7	8	9
Correlation peak (x100)	1.3	2.7	5.5	11	22	44	88	177	354
Result	✓	✓	✓	✓	✓	✗	✗	✓	✓

were conducted with two O-RUs set up, and we only controlled O-RU2, the registration was successful in scenarios 1, 2, and 4, indicating that the UE can register through path ⓑ as signal blocking occurred in path ⓐ. In scenario #3, registration was not always successful; it sometimes failed or required multiple retries and a longer wait time to succeed.

Further analysis of this case reveals that the correlation peak value is crucial for 5G preamble detection. In Fig. 6.b, the UE sends a preamble index with a peak value (index, peak). In path ⓐ, the preamble is compromised and altered to (index1, peak1). Therefore, the 5G system receives two correlation peaks, each corresponding to a different index, e.g., (index1, peak1) and (index, peak). The preamble detection is related to the correlation peak, if the difference between peak and peak1 is not significant, the lower index is usually detected as the received preamble index from the observation. Therefore, if (peak, index) is detected, then the registration is successful, but if (peak1, index1) is detected, then UE will retry by ramping up the power, which results in a higher correlation peak and makes path ⓑ more easily detected and successfully registered. In this procedure, we can observe numerous RARs with incorrect RAPID values. Registration is only successful if the RAPID matches the intended index.

2) Experiment 2: Longer registration times or occasional registration failures do not meet our requirements. Upon further investigation of the correlation peak's impact, we discovered an intriguing situation. We generated multiple fake preambles with the same preamble index, incrementally increasing the correlation peak by raising all PRBs' exponent value (refer to the arrow in Fig. 11) from 1 to 9 . Table II demonstrates the result of attacks.

As the exponent value increases, the correlation peak also rises. Table II shows that when the peak value ranges from 4400 to 8800, the UE will fail to register. When analyzing the eCPRI packets, unlike scenario #3 in experiment 1 where numerous RARs were observed, increasing the exponent to a certain value in this experiment results in no RAR responses from the 5G system. The 5G system can no longer recognize the fake preamble, even when a legitimate preamble is received from path ⓑ simultaneously. This observation allows us to control a single O-RU, which then affects the other O-RUs and results in registration failure.

3) Experiment 3: In previous experiment, we placed the UE close to both O-RUs so that both could receive similar preambles. As a result, O-RU2 under my control was able to receive all the preambles, and the compromised RU could identify all the preambles using the occasion plus circular checking method. This made the attack successful, causing the UE to fail to register. However, if the UE is far from O-RU2, O-RU2 may not receive all preambles sent by the UE, allowing the UE to successfully register through O-RU1. To counter this, we can replace all packets that match the preamble occasion with fake preambles. The tradeoff is that many preambles will be observed even when no UE is trying to connect, which may appear suspicious.

D. Countermeasures

To mitigate the 5G-Muffler attacks, we propose several countermeasures. For *5G-Muffler-1*, hardening the access control to the O-FH switch can prevent unauthorized manipulation. Additionally, adding integrity protection to the IQ data in the eCPRI or lower layers, potentially using MACsec, ensures that a MitM device cannot tamper with the MAC layer frames. For *5G-Muffler-2*, performing sanity checks on the IQ samples before aggregation to ensure they fall within the correct range can enhance security. Furthermore, in cells with multiple O-RUs, using selected trusted O-RUs to generate PRACH preambles and verifying their correct reception at the O-DU can protect against the attack.

Other potential countermeasures include implementing robust monitoring and anomaly detection systems specifically for the O-FH interface to quickly identify and respond to suspicious activities. Regular security audits and updates to the O-FH configuration and access controls can also help maintain a secure environment. These measures collectively strengthen the security of the O-FH interface and defend against covert DoS attacks.

VII. CONCLUSION AND FUTURE WORK

We presented 5G-Muffler, a set of covert DoS attacks on the open fronthaul interface. To be stealthy, 5G-Muffler targets the random access procedure, which is the first step for a UE to connect to a network. We described two variants of 5G-Muffler under two different threat models. In *5G-Muffler-1*, the attacker can manipulate the O-FH switch settings and access devices attached to the switch to launch a Man-In-The-Middle attack and modify eCPRI traffic. In *5G-Muffler-2*, the attacker manipulates one O-RU in a multi-O-RU cell setup, exploiting weaknesses in signal aggregation to DoS all UEs trying to connect to the cell. We demonstrated 5G-Muffler on commercial O-RAN systems and proposed countermeasures to mitigate these attacks.

Future work. In the future, we aim to implement and evaluate the proposed countermeasures, such as hardening access controls to the O-FH switch, adding integrity protection to IQ data using protocols like MACsec, and performing sanity checks on IQ samples before aggregation. Additionally, in cells with multiple O-RUs, we plan to use selected trusted O-RUs to generate PRACH preambles and verify their correct reception at the O-DU. This will help us assess the practical effectiveness of these measures and further enhance the security of the O-FH interface. By continuously improving these defenses, we aim to provide robust protection against covert DoS attacks in the evolving O-RAN ecosystem.

REFERENCES

[1] O-RAN Alliance, "O-RAN Alliance," https://www.o-ran.org/.

[2] M. Polese, L. Bonati, S. D'oro, S. Basagni, and T. Melodia, "Understanding o-ran: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1376–1411, 2023.

[3] O-RAN Alliance, "O-RAN Control, User and Synchronization Plane Specification," O-RAN Alliance, Technical Report, Jun 2024.

[4] ——, "O-RAN Study on Security for Fronthaul CUS-Plane," O-RAN Alliance, Technical Report, Jun 2024.

[5] S.-H. Liao, C.-W. Lin, F. A. Bimo, and R.-G. Cheng, "Development of c-plane dos attacker for o-ran fhi," in *Proc. of the 28th Annual International Conference on Mobile Computing and Networking (MobiCom)*, July 2022, pp. 850–852.

[6] H. Wen, P. Porras, V. Yegneswaran, A. Gehani, and Z. Lin, "5g-spector: An o-ran compliant layer-3 cellular attack detection service," in *Proc. of the 31st Annual Network and Distributed System Security Symposium (NDSS '24)*, San Diego, CA, USA, 2024.

[7] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5greasoner: A property-directed security and privacy analysis framework for 5g cellular network protocol," in *Proc. of the ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 669–684.

[8] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on lte," in *Proc. 28th USENIX Security Symposium (USENIX Security 19)*, 2019.

[9] 3GPP, *Security architecture and procedures for 5G System*, 3rd Generation Partnership Project (3GPP) Std. TS 33.501, Mar 2024, release 15.

[10] H. Kim, J. Lee, E. Lee, and Y. Kim, "Touching the untouchables: Dynamic security analysis of the lte control plane," in *Proc. IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2019, pp. 1153–1168.

[11] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "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*, 2019, pp. 669–684.

[12] O-RAN Alliance, "O-RAN Conformance Test Specification," O-RAN Alliance, Technical Report, Jun 2024.

[13] ——, "O-RAN Security Threat Modeling and Risk Assessment," O-RAN Alliance, Technical Report, Jun 2024.

[14] ——, "O-RAN Security Tests Specifications," O-RAN Alliance, Technical Report, Jun 2024.

[15] ——, "O-RAN Security Requirements and Controls Specifications," O-RAN Alliance, Technical Report, Mar 2022.

[16] D. Dik and M. S. Berger, "Transport security considerations for the open-ran fronthaul," in *Proc. IEEE 4th 5G World Forum (5GWF)*, Montreal, QC, Canada, 2021, pp. 253–258.

[17] O-RAN Alliance, "O-RAN Fronthaul Interoperability Test Specification," O-RAN Alliance, Technical Report, Jun 2024.

[18] W. Azariah, F. A. Bimo, C.-W. Lin, R.-G. Cheng, N. Nikaein, and R. Jana, "A survey on open radio access networks: Challenges, research directions, and open source approaches," *Sensors*, vol. 24, no. 3, p. 1038, 2024.

[19] O-RAN Alliance, "O-RAN Xhaul Packet Switched Architectures and Solutions," O-RAN Alliance, Technical Report, Jun 2024.

[20] D. Mimran, R. Bitton, Y. Kfir, E. Klevansky, O. Brodt, H. Lehmann, Y. Elovici, and A. Shabtai, "Evaluating the security of open radio access networks," *arXiv preprint arXiv:2201.06080*, 2022.

[21] F. Klement, S. Katzenbeisser, V. Ulitzsch, J. Krämer, S. Stanczak, Z. Utkovski, I. Bjelakovic, and G. Wunder, "Open or not open: Are conventional radio access networks more secure and trustworthy than open-ran?" *arXiv preprint arXiv:2204.12227*, 2022.

[22] A. Grassi, G. Piro, and G. Boggia, "A look at random access for machine-type communications in 5th generation cellular networks," *Internet Technol. Lett.*, vol. 1, no. 1, p. e3, 2017.

[23] 5g rach in details. [Online]. [Online]. Available: https://www.sharetechnote.com/html/5G/5G_RACH.html

[24] D. Chu, "Polyphase codes with good periodic correlation properties (corresp.)," *IEEE Transactions on Information Theory*, vol. 18, no. 4, pp. 531–532, 1972.