IEEE Open Journal of the Communications Society

Received XX Month, XXXX; revised XX Month, XXXX; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version 11 January, 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.011100

Conformance Testing of F1AP Protocol in 5G O-RAN

CHENG-FENG HUNG[1] (Member, IEEE), SHIH-HSIUNG CHANG[2], TSUNG-YEN HSIEH[2], SHIN-MING CHENG[2] (Member, IEEE), TAO BAN[1] (Member, IEEE), TAKESHI TAKAHASHI[1] (Senior Member, IEEE)

[1]Cybersecurity Research Institute, National Institute of Information and Communications Technology, Tokyo, Japan
[2]National Taiwan University of Science and Technology, Taipei, Taiwan

CORRESPONDING AUTHOR: C.-F. Hung (e-mail: hungchengfeng@nict.go.jp)

This work was partially supported by the National Science and Technology Council (NSTC), Taiwan, under Grant 113-2221-E-011-156-MY3 and 113-2221-E-011-157-MY3.

ABSTRACT The rapid development of fifth-generation (5G) communication networks is driven not only by the standardization efforts of the 3rd Generation Partnership Project (3GPP), but also by the modular, interoperable design introduced by the Open Radio Access Network (O-RAN) architecture. While O-RAN facilitates multi-vendor integration through open interfaces, it raises significant security and interoperability concerns, particularly when third-party components, such as the O-RAN Central Unit (O-CU), do not fully comply with protocol specifications. To address this challenge, we propose a conformance testing mechanism integrated into the O-RAN Distributed Unit (O-DU) that analyzes packet content and verifies the signaling behavior of newly introduced O-CUs before deployment. By proactively inspecting the F1 Application Protocol (F1AP) messages exchanged between the O-CU and O-DU, the mechanism prevents non-compliant signaling sequences and malformed messages from impacting live network operations. We implement this testing framework on a 5G standalone (SA) platform using OpenAirInterface (OAI). We simulate various abnormal F1AP scenarios, including incorrect message sequences and unauthorized field modifications in RRC and NAS payloads. Experimental results demonstrate that the proposed mechanism can detect such anomalies with high effectiveness and incurs only minimal latency overhead, offering a practical pre-deployment safeguard to enhance the security and reliability of O-RAN systems.

INDEX TERMS Conformance Testing, F1AP, O-RAN Security, State Machine, 5G

I. INTRODUCTION

THE rapid evolution of fifth-generation (5G) services imposes stringent performance requirements, such as high bandwidth and ultra-low latency. However, traditional telecom networks, dominated by proprietary vendors, are inherently inflexible, which impedes timely deployment and scalable upgrades [1], [2]. The O-RAN Alliance proposed a disaggregated Radio Access Network (RAN) architecture to overcome these limitations. This architecture decouples the functions of traditional base stations into the O-RAN Central Unit (O-CU), O-RAN Distributed Unit (O-DU), and O-RAN Radio Unit (O-RU), enabling interoperability across multi-vendor environments. These components communicate through standardized interfaces, including E2, A1, O1, R1, and the Open Fronthaul Interface (O-FHI), as illustrated in Fig. 1. In addition, O-RAN incorporates two RAN Intelligent Controllers (RICs) to manage and optimize RAN operations dynamically, thereby improving overall network performance [2], [3]. The disaggregated design introduces new security and interoperability challenges despite its architectural flexibility. In particular, white-box vendors may fail to fully adhere to 3GPP and O-RAN specifications, resulting in malformed signaling sequences or protocol violations [4]. [5] proposed an application scheme for placing detection elements within the RAN, while [6], [7] further explored the feasibility of implementing conformance testing mechanisms for the NG Application Protocol (NGAP) and E2 interfaces in an O-RAN environment. More critically, conformance issues at the O-CU level can propagate throughout the network, disrupting O-DU and O-RU communication. Such

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

disruptions may lead to service unavailability and compromise the integrity of end-to-end 5G connections.

In the O-RAN architecture, the O-CU is responsible for handling the workloads of the Radio Resource Control (RRC), Service Data Adaptation Protocol (SDAP), and Packet Data Convergence Protocol (PDCP) layers, thereby facilitating the connection of user equipment (UE) to the 5G core network. The O-CU and the O-RAN Distributed Unit (O-DU) exchange F1 Application Protocol (F1AP) messages over the F1 interface to support security authentication between the UE and the core network, as well as to enable service migration, offloading, and handover procedures when the UE connects to a base station. Currently, for the security protection of F1AP messages, the 3GPP specifications [8], [9] recommend using encryption technologies such as DTLS or IPsec to protect F1AP packets. However, these specifications are not mandatory in all deployments. The threat modeling document from O-RAN WG11 [4] also identifies the absence of DTLS or IPsec protection as a potential threat. Multi-vendor O-CU implementations provide greater flexibility in O-RAN deployment but also introduce interoperability and security risks. Suppose an O-CU's F1AP processing deviates from the 3GPP or O-RAN specifications. In that case, it may transmit abnormally ordered or malformed messages to the O-DU, disrupting UE context management and preventing stable attachment. Therefore, before integrating new O-CUs into the operator's network, it is essential to verify their signaling compliance. This necessity motivates the proposed pre-deployment conformance testing mechanism, which inspects F1AP message behavior to ensure alignment with standardized procedures before deployment.

To address this gap, we propose a conformance testing mechanism deployed at the O-DU to inspect F1AP messages sent by the O-CU. Given the critical role of F1AP in UE registration and mobility management, this mechanism ensures that third-party O-CUs conform to standardized signaling behavior before deployment. By incorporating protocol-specific finite-state machines (FSMs) to model expected signaling sequences across the F1AP, RRC, and NAS layers, the design effectively detects procedure-order violations via stateful F1AP semantics, identifies cross-layer inconsistencies between F1AP and embedded RRC messages, and recognizes NAS-level anomalies propagated through F1AP encapsulation. Operationally, the conformance tester records the current protocol state upon receiving signaling messages and enumerates all valid subsequent messages based on the FSM definitions. Any incoming message that does not follow these defined transition paths is immediately flagged as non-compliant or potentially malicious. Meanwhile, the system inspects individual packet fields in parallel to identify malformed content or tampered parameters.

To evaluate the proposed framework, we implemented a 5G Standalone (SA) testbed using OpenAirInterface (OAI). We inserted a malicious module at the O-CU front end to generate abnormal F1AP behavior, and the O-DU ran our conformance testing mechanism. Through this testbed, we assess whether the proposed semantic validation mechanism can effectively detect procedure-level inconsistencies, cross-layer RRC deviations, and NAS-related anomalies introduced by non-compliant O-CUs. In contrast to existing NGAP or RRC/NAS detection tools, our approach performs pre-deployment verification of F1AP procedures from the O-DU side. It enforces stateful message sequencing and protocol field correctness as defined in 3GPP TS 38.473 [10]. We constructed three experimental scenarios that represent unexpected F1AP sequences, abnormal RRC parameters encapsulated in F1AP, and anomalous NAS parameters carried within F1AP. These scenarios demonstrate the framework's ability to identify protocol deviations produced by non-compliant O-CU implementations. The results show that the mechanism detects all anomalies while adding only about 11 ms of additional connection latency, which remains within 5G control-plane requirements. By validating protocol compliance before integration, the proposed approach prevents incorrectly implemented O-CUs from disrupting O-CU and O-DU interoperability. It improves the reliability of multi-vendor O-RAN deployments.

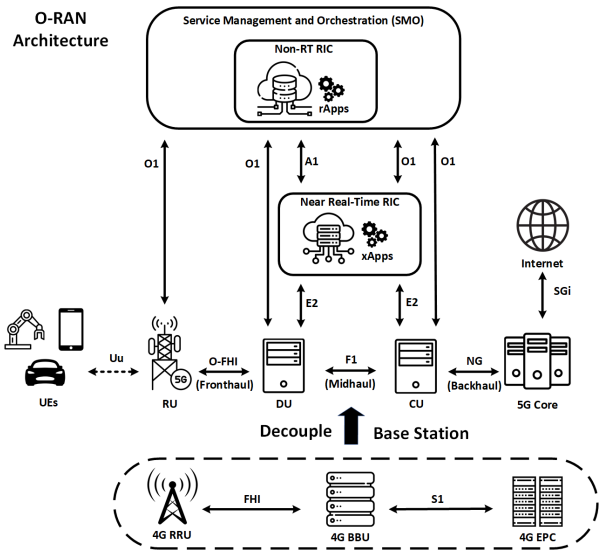


FIGURE 1. O-RAN Architecture

The structure of this paper is organized as follows: Section II introduces the overall architecture of 5G O-RAN and provides a detailed explanation of the F1AP operation process, along with the potential threats associated with it. Section III presents the design of the proposed conformance testing mechanism. Section IV elaborates on the underlying design principles and the threat model. Section V describes the experimental environment and provides an in-depth analysis of the proposed method through three research questions. Finally, Section VI concludes the paper.

II. BACKGROUND KNOWLEDGE

A. 5G O-RAN ARCHITECTURE

Fig. 1 illustrates the functions of each component and the corresponding protocol layers they are responsible for after the base station is decoupled.

- User Equipment (UE): User devices such as smartphones, computers, and IoT terminals connect to the 5G network by initiating a registration procedure with the core network. The process begins when the device establishes an RRC connection with the RAN and then sends its subscription credentials, including the Subscription Concealed Identifier (SUCI), to the core network for authentication.
- O-RAN Radio Unit (O-RU): The O-RU performs low-PHY and radio-frequency functions and connects to the O-DU through the Open Fronthaul interface [11]. The O-FHI carries IQ user-plane samples and PHY control information, including beamforming, timing, and synchronization parameters. It does not transport any F1AP, RRC, or NAS signaling. As a result, the O-RU does not participate in CU–DU control-plane procedures or upper-layer protocol processing.
- O-RAN Distributed Unit (O-DU): The O-DU is a critical logical node in wireless communication networks, primarily responsible for handling functions across multiple protocol layers, including Radio Link Control (RLC), Medium Access Control (MAC), and Physical Layer-High (PHY-High). The RLC layer provides logical control over wireless connections, ensuring reliable data transmission and connection management. The MAC layer operates between the RRC and PHY layers, coordinating and allocating radio resources to maintain efficient communication. The PHY-High layer handles advanced physical layer operations, such as signal modulation, demodulation, and error correction. The O-DU establishes connections with the Service Management and Orchestration (SMO) framework, the O-CU, the Near-Real-Time RAN Intelligent Controller (Near-RT RIC), and the O-RU via the O1, F1, E2, and FHI, respectively. Distributed applications (dApps) can be deployed on the O-DU to provide intelligent control and enhance overall network performance [3], [12], [13]. Although the Near-RT RIC enables network control closer to the edge, data transmission via the E2 interface still introduces latency and overhead. By executing dApps directly on the O-DU, real-time data processing and localized control can be achieved, significantly reducing the delay and signaling burden associated with data round-trips [12].
- O-RAN Central Unit (O-CU): The O-RAN Central Unit (O-CU) plays a crucial role in the O-RAN architecture by executing decoupled base station functionalities that were traditionally handled in monolithic systems. Specifically, the O-CU is responsible for upper-layer protocol operations, including the RRC, SDAP, and PDCP. It is logically divided into two components: the O-CU Control Plane (O-CU-CP) and the O-CU User Plane (O-CU-UP) [11]. The O-CU-UP processes the SDAP and PDCP-UP layers. SDAP is responsible for maintaining quality-of-service (QoS) differentiation across multiple services. At the same time, PDCP-UP ensures the integrity, confidentiality, and transmission efficiency of user plane data by applying functions such as header compression and encryption. In parallel, the O-CU-CP handles signaling control by managing the RRC and PDCP-CP layers. The RRC layer configures and maintains radio bearers and mobility procedures, whereas PDCP-CP supports control-plane data integrity and state management.
  Regarding network connectivity, the O-CU interfaces with the O-DU, the SMO framework, and the Near-Real-Time RIC through the F1, O1, and E2 interfaces. It also performs critical computing tasks that would otherwise be distributed to the O-DU in traditional architectures, serving as a central hub between the DUs and the 5G core network. Importantly, a single O-CU may manage multiple O-DUs and their corresponding O-RUs via the midhaul interface. Suppose a malfunction occurs in the O-CU due to implementation defects, protocol misconfigurations, or malicious behavior. In that case, it may lead to a loss of connectivity across a wide range of dependent network elements. This could result in a large-scale service disruption, significantly degrading network availability and user experience. Therefore, ensuring the O-CU's operational correctness and compliance with protocols is essential to maintaining the reliability and stability of O-RAN systems.
- Core Network: The core network primarily provides users with internet access and related management services. Its key components include the Access and Mobility Management Function (AMF), the Network Repository Function (NRF) for control plane operations, and the User Plane Function (UPF) for handling user plane data. This paper focuses on the AMF, which is central to maintaining network efficiency by managing UE connections, overseeing registration and authentication procedures, and handling mobility-related services. Once the AMF successfully authenticates the UE, it establishes a NAS connection with the UE and exchanges encrypted and integrity-protected signaling messages to ensure secure communication.

B. F1 APPLICATION PROTOCOL (F1AP)

- F1AP Interface Network Flow:
  The F1 interface is a functional split interface between the O-CU and O-DU, standardized by 3GPP for 5G New Radio (NR) as defined in [8], [10], [14], [15]. It ensures interoperability between network components developed by different vendors. The F1 interface con-

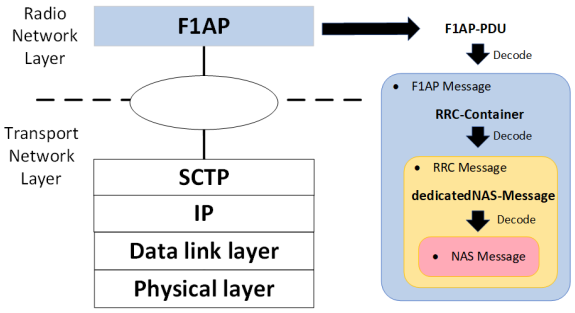


FIGURE 2. F1AP Protocol Structure

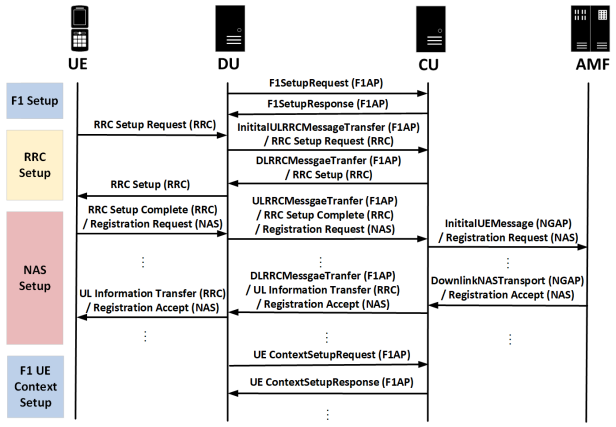


FIGURE 3. F1AP Message Flow

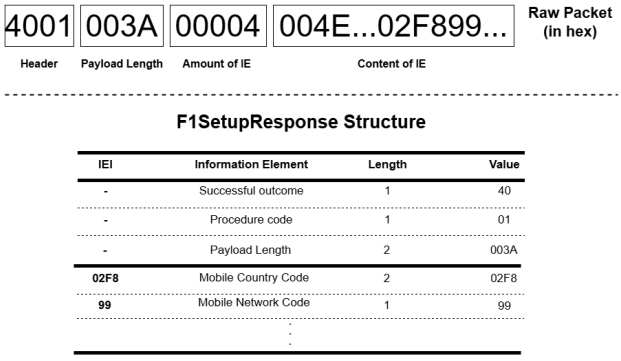


FIGURE 4. F1AP Payload Schematic

sists of two sub-interfaces: the Control Plane (F1-C) and the User Plane (F1-U). The F1AP operates over the F1-C interface and manages signaling procedures, including UE context management, configuration updates, and mobility control. This paper primarily focuses on F1AP and its role within the F1-C plane. F1AP is an application-layer protocol that runs on top of the Stream Control Transmission Protocol (SCTP) and provides the transport layer. It facilitates signaling exchange between the O-CU and O-DU to coordinate and manage radio interface operations. Within the F1AP messages, the O-CU and O-DU encapsulate information from the RRC and NAS layers. Core F1AP functions include establishing, modifying, and releasing radio bearers, as well as reconfiguring radio resources. It also supports mobility-related operations such as inter-DU UE handovers, ensuring seamless connectivity as the UE moves across cells. Additionally, F1AP enables the management of various radio resource control and QoS parameters, contributing to robust and flexible network operation.

Fig. 3 illustrates the signaling procedure for UE registration to the 5G Core Network within the O-RAN architecture. The registration process involves multiple protocol layers, including F1AP between the O-DU and O-CU, RRC between the UE and O-DU, and NAS messages exchanged between the UE and the AMF via the NGAP interface. The figure highlights key signaling stages, including F1 setup, RRC connection establishment, NAS registration, and UE context setup, all of which are essential for successful UE attachment to the 5G core network.

- F1AP Packet

  Most control plane messages in F1AP are transmitted in plaintext between the O-CU and O-DU before the completion of encryption and authentication through the 5G Authentication and Key Agreement (AKA) procedure, which is part of the NAS protocol [16]. F1AP messages encapsulate control plane protocol layer information, including RRC and NAS messages, as illustrated in Fig. 2. By deconstructing and analyzing the contents of F1AP Protocol Data Units (PDUs), the transmitted F1AP service information can be extracted, as shown in Fig. 4.

  A detailed examination of these messages reveals multiple Information Elements (IEs), among which the *RRC-Container* is particularly important. This field contains the complete RRC layer payload, representing RRC messages exchanged between the O-CU and the UE, as depicted in Fig. 5. Since the O-DU does not need to interpret the RRC PDU embedded in the *RRC-Container*, this field can be directly parsed to extract the full RRC message. As previously mentioned, before establishing a secure channel between the UE and the network, these F1AP messages are transmitted in plaintext. Once the RRC connection between the UE and O-CU is established, it becomes possible to analyze the RRC content to extract security-related parameters, such as the UE's supported encryption and integrity protection algorithms.

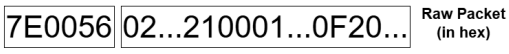
  The RRC message may also contain the *dedicatedNAS-Message* field, which carries the complete NAS message payload. This payload remains plaintext until the UE completes the 5G AKA authentication procedure. Therefore, the *dedicatedNAS-Message* can be directly analyzed to retrieve the NAS message content, as illustrated in Fig. 6. The NAS layer is the commu-

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2025.3649885

Security Mode Command Structure

IEI	Information Element	Length	Value
-	Sequence Number	2	0002
-	Message Type	1	20
0810	Security algorithm config	2	0810
-	MAC parameters	4	090A776B

FIGURE 5. **RRC Payload Schematic**



Authentication Request Structure

IEI	Information Element	Length	Value
-	5G mobility management	1	7E
-	Security header type	1	00
-	Authentication request	1	56
21	Element ID	1	21
00...0F	RAND value	16	00...0F
	. . .		

FIGURE 6. **NAS Payload Schematic**

nication interface between the UE and the Access and Mobility Management Function (AMF). During NAS connection establishment, these messages include authentication-related parameters, such as the random number (RAND) and the authentication token (AUTN), which the core network uses to verify the UE's identity.

- F1AP Possible Security Problem: F1AP operates over SCTP, which lacks built-in data protection mechanisms. Although 3GPP TS 33.501 [9] recommends using IPsec ESP with IKEv2 to secure F1-C transmissions, this recommendation is not mandatory for network operators. To meet security requirements related to data confidentiality and integrity, an additional secure transport layer should be established between the O-CU and the O-DU. In the context of the O-RAN architecture, the O-RAN Working Group 11 (WG11) specification [17] explicitly recommends encryption mechanisms, such as IPsec and DTLS, to protect communication between the O-CU and O-DU. However, many open-source implementations and third-party O-CU products have not yet adopted these security measures. Moreover, due to varying levels of development maturity and compliance testing, third-party O-CUs may exhibit non-compliant signaling behaviors that deviate from 3GPP or O-RAN specifications. These deviations increase the risk of protocol-level inconsistencies and security vulnerabilities. Without sufficient protection and verification, an attacker could exploit a misconfigured or compromised O-CU to act as a malicious relay and infiltrate the core network. Furthermore, adversaries may launch denial-of-service (DoS) attacks to disable the O-DU within a targeted region, disrupting local network services and undermining system availability.

C. SECURITY THREAT BEHIND DECOUPLED 5G O-RAN BASE STATION

By introducing Network Function Virtualization (NFV) and the F1 interface, the O-RAN architecture disaggregates traditional monolithic base station equipment into software-defined components, namely the O-CU and O-DU. This modularization lowers entry barriers and enables vendors and enterprises of varying scales to participate in the O-RAN ecosystem [18]. In this context, telecom equipment manufacturers can develop white-box O-CU and O-DU hardware and software that comply with the F1AP message specifications. Furthermore, O-RAN envisions diverse white-box hardware designs tailored to various base station deployment scenarios to improve spectral efficiency, enhance energy efficiency, and reduce deployment costs [19]. As more third-party components are integrated into the system, comprehensive threat analysis and corresponding security countermeasures become essential to defend against potential attacks that may exploit newly introduced interfaces and functionalities [7], [20]–[25].

On the other hand, multi-vendor deployments may introduce interoperability issues among components. If white-box base station equipment lacks systematic coordination and rigorous pre-validation of its messaging services, the O-CU and O-DU may fail to communicate correctly via F1AP messages. Such deficiencies can prevent UE from completing secure registration with the core network after connecting to the base station, thereby degrading the overall 5G network's performance and reliability. Therefore, it is imperative to validate the messaging services of each component before base station integration to avoid communication anomalies caused by implementation flaws [18]. Within the O-RAN architecture, the O-CU plays a critical role in handling F1AP signaling and is required to interface with multiple O-DUs concurrently in commercial deployments. Consequently, ensuring the security and protocol compliance of the O-CU is of paramount importance [26], [27].

D. RELATED WORK

The O-RAN Alliance has identified a broad set of security concerns associated with O-CU components and has published corresponding testing and threat-model guidelines [4], [28], as well as methodologies for constructing packet-capture frameworks for open interfaces [29]. Complementing O-RAN specifications, 3GPP defines the signaling procedures for RRC and NAS [30], [31] and establishes a range of architecture- and message-layer security requirements for the 5G RAN [9], [32]–[35]. These specifications emphasize the RAN's critical role in handling control-plane traffic between the UE and the 5G Core and motivate the need to

ensure signaling correctness and robustness in disaggregated deployments.

Existing conformance and analysis tools address different protocol boundaries and deployment scenarios within the 5G O-RAN architecture. Lin et al. [7] propose NGAP conformance testing between the O-CU and the 5GC via MEC-based packet inspection, but do not report quantitative performance metrics, such as detection rate, latency, or processing overhead, which prevents a meaningful numerical comparison. 5G-Spector [24] offers a comprehensive control-plane analysis framework for O-RAN, achieving nearly 100% detection accuracy with less than 2% CPU utilization and under 100 MB of memory overhead. Still, it incurs 140–280 ms of detection latency and targets runtime RRC/NAS exploit detection rather than protocol-level conformance.

Recent research has addressed security across various O-RAN interfaces. Groen et al. [27] evaluated IPsec- and MACsec-based protection on the E2 interface and Open Fronthaul links to quantify the encryption overhead. Hung et al. [36] examined E2 security by analyzing xApp access-control and signaling vulnerabilities. In contrast, Thimmaraju et al. [37] investigated Near-RT RIC and A1 interface testing, focusing on policy behavior. However, these efforts primarily target encryption mechanisms and RIC policies rather than protocol consistency on the CU–DU boundary. Existing solutions, including NGAP-focused schemes [7] and runtime intrusion detection systems such as 5G-Spector [24], do not specifically validate the stateful F1AP procedures defined in 3GPP TS38.473 [10]. Consequently, vendor-specific O-CU implementations currently lack sufficient verification for F1AP compliance before deployment. Our work addresses this gap by introducing a pre-deployment conformance testing mechanism at the O-DU. Distinguished from runtime solutions that rely on resource-intensive packet inspection, our approach enforces deterministic stateful checking of F1AP message sequencing and field correctness while keeping the impact on connection latency minimal. The detailed performance evaluation is presented in Section V.

III. CONFORMANCE TESTING MECHANISM

As summarized in Section II-D, existing security and conformance approaches target different stages of the O-RAN deployment lifecycle. NGAP-based validation strengthens the core-facing O-CU–5GC interface, while runtime analysis frameworks such as 5G-Spector monitor RRC and NAS signaling on the UE-facing interface. E2- and A1-focused studies further enhance RIC-driven control and policy behavior. These approaches operate at different protocol boundaries and deployment phases, but none validate the DU-facing F1AP behavior of O-CUs before integration. In disaggregated, multi-vendor O-RAN systems, improper or non-compliant F1AP implementations may remain undetected by NGAP- or RRC/NAS-based mechanisms yet still disrupt UE context establishment on the DU side, motivating the need for dedicated pre-deployment validation at the O-DU.

Although production-grade O-CUs perform internal consistency checks, these checks focus mainly on local schema correctness, such as ASN.1 structure, mandatory information-element presence, and vendor-specific rules, and do not ensure procedure-level conformance from the O-DU perspective. F1AP procedures are stateful: each message must appear in the correct phase of the UE lifecycle, remain consistent with previously exchanged parameters, and preserve cross-layer bindings among F1AP, RRC, and NAS information elements. Schema validation or isolated CU-side checks cannot verify these properties. To close this gap, we introduce a pre-deployment conformance testing mechanism on the O-DU to validate O-CU protocol compliance in disaggregated RAN deployments, as shown in Fig. 7. The O-DU and O-RU in our testbed operate according to the baseline specifications defined in 3GPP TS 38.470, TS 38.472, and TS 38.473, while following the architectural guidelines provided by O-RAN Alliance documents [8], [10], [11], [14].

The conformance testing mechanism in this work builds directly on the 3GPP F1AP specifications (3GPP TS 38.470–38.473) [8], [10], [14], [15], which define the message formats and procedures of the CU–DU interface. Although 3GPP TS 33.523 [38] outlines robustness testing requirements for commercial O-CU products and references the generic fuzzing framework in 3GPP TS 33.117 [39], these methods primarily target syntax-level mutations and do not examine procedure ordering or cross-layer parameter consistency. Our mechanism complements these techniques by introducing stateful and semantically informed checks on F1AP behavior. It performs three types of validation: (1) verifying message sequences using FSMs derived from 3GPP, (2) checking parameter consistency across F1AP and RRC layers, and (3) validating NAS-related information encapsulated within F1AP messages. This approach goes beyond schema-level checks and provides practical assurance of F1AP correctness in multi-vendor O-RAN deployments. Furthermore, because both the O-CU and O-DU in our testbed remain unmodified and all message perturbations occur solely at the F1 interface, the mechanism inherently follows a black-box interface-testing methodology, consistent with how operators evaluate third-party O-CUs without requiring re-implementation of CU/DU internals [39].

The proposed conformance testing architecture consists of the following three main components:

- **O-CU:** Responsible for generating and transmitting legitimate control plane and user plane traffic in accordance with 3GPP and O-RAN specifications while maintaining communication with the O-DU.
- **Malicious Component:** Positioned between the O-CU and O-DU, this component intercepts legitimate packets from the O-CU, mutates their contents, and forwards the modified versions to the O-DU to evaluate the robustness of the detection mechanism.

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2025.3649885

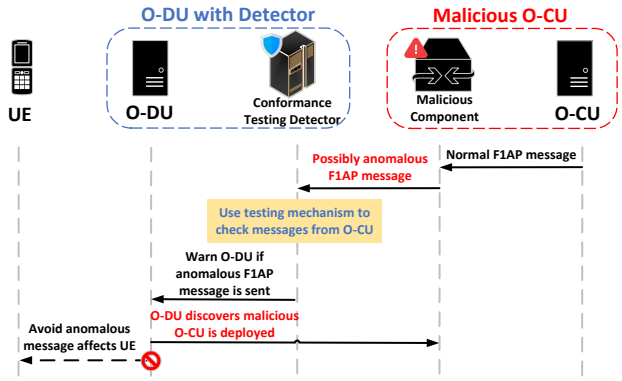


FIGURE 7. System Model Architecture

- **Conformance Testing Detector:** A critical verification module deployed on the O-DU that inspects F1AP, RRC, and NAS messages to assess protocol compliance and detect non-compliant behavior or potential attacks.

A. VERIFYING MESSAGE PATHS USING FINITE STATE MACHINE

After the conformance testing mechanism intercepts the F1AP packets sent by the O-CU, it first deconstructs them to extract the relevant F1AP information. This process includes parsing the F1AP payload and decoding its hexadecimal content. As shown in Fig. 4, each packet contains a header that identifies the F1AP message type. By referencing the 3GPP specifications, the system determines the message type based on this header value; for example, 4001 corresponds to *F1SetupResponse*, and 0005 corresponds to *UEContextSetup*. The decoded payload also includes essential fields such as the *RRC-Container* and *DedicatedNAS-Message*, which encapsulate the RRC and NAS layer messages. Abnormalities in these control plane messages may cause service disruptions on the F1 interface. Therefore, the mechanism analyzes the contents of the RRC and NAS payloads to determine the message types being transmitted. Based on the payload analysis shown in Fig. 5, the system identifies the current RRC message using the PDCP and RRC headers within the RRC payload. For example, the header value 00020 indicates a *Security Mode Command*. Similarly, as shown in Fig. 6, the system identifies the current NAS message using the NAS header within the NAS payload; for instance, 7E0056 indicates an *Authentication Request*. Once the RRC and NAS message types are identified, the conformance testing mechanism uses the FSM to evaluate whether the current F1AP message sequence is valid or anomalous.

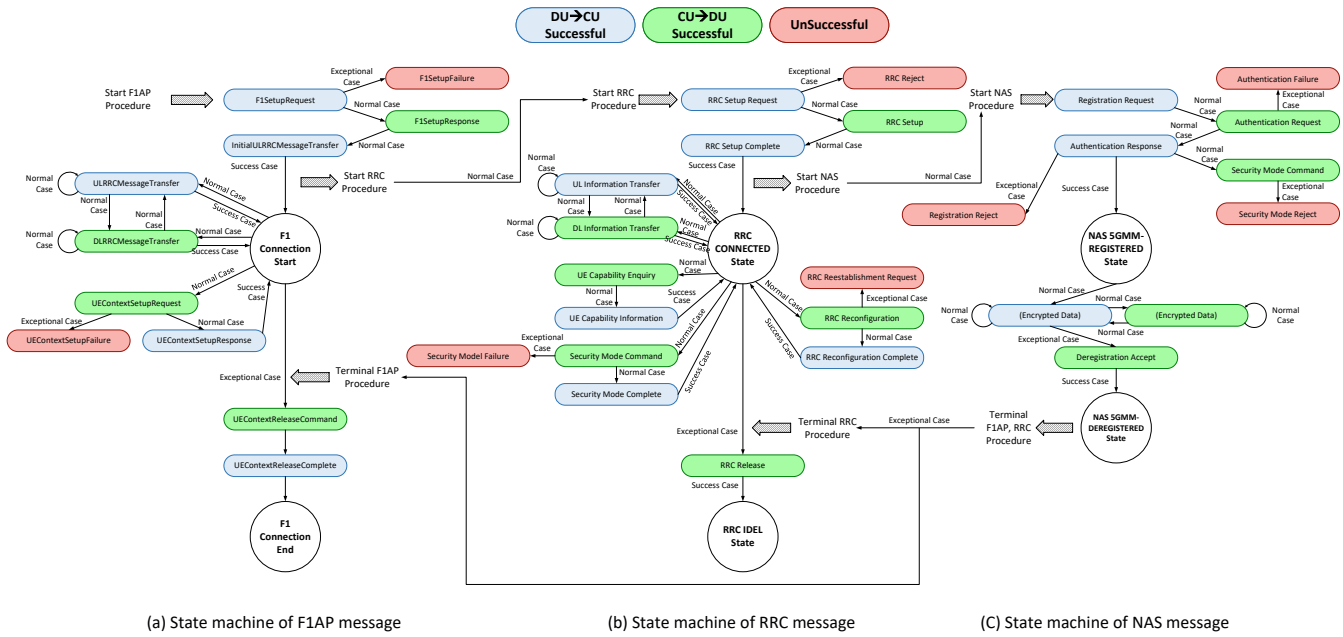
The FSMs used in this mechanism are constructed based on observed legitimate F1AP message flows. The FSMs are categorized into three types according to the protocol layer involved: (1) checking the state of F1AP messages, (2) checking the state of RRC messages encapsulated within F1AP, and (3) checking the state of NAS messages encapsulated within F1AP. The complete FSM diagrams are shown in Fig. 8. The FSM operates according to the following formal definition. We define the FSM as $G = \{V, E\}$, where V is the set of vertices and E is the set of directed edges. The set V includes square nodes, which represent the characteristics of messages received by the testing mechanism and are categorized into successful and unsuccessful message types. It also includes circular nodes that represent the current connection states of the protocol. These states help determine whether a given message is consistent with the expected connection state. Each directed edge e_{ij} represents a valid state transition from node v_i to node v_j, where v_i, $v_j \in V$. The label on edge e_{ij} indicates the reason or condition that triggers the transition between these two states.

When the testing mechanism begins parsing a message v_j, it uses the message header to determine its characteristics. If the current message type and connection state match the expected transition defined in the FSM, the message is considered valid, and the flow proceeds as intended. However, if this condition is violated, the FSM determines that the message is anomalous, meaning the current transition $e_{ij} \notin E$, and the O-DU is notified accordingly. If the message follows a valid transition path, i.e., $e_{ij} \in E$, the testing mechanism proceeds to the second stage.

B. VERIFYING SETTINGS WITHIN THE F1AP AND RRC MESSAGES

In the second stage of the testing mechanism, the system verifies whether the configurations within the F1AP and RRC messages sent from the O-CU are correctly set. These two message types contain fields within the O-CU's authorized control scope, and many of these fields are interrelated with parameters in previously transmitted F1AP messages. Therefore, consistency checks across related message instances are required to validate protocol compliance. As discussed in Section 3, the F1AP message payload includes various IEs and the message header. As shown in Fig. 4, IEs encapsulate multiple telecommunications service parameters, including the UE's PLMN ID. Moreover, Fig. 5 and Fig. 6 illustrate that the IEs also contain security-related fields, including *securityAlgorithmConfig* in the RRC layer and *UESecurityCapability* in the NAS layer. These fields are critical for validating the integrity of F1AP and RRC signaling content.

Upon receiving a valid F1AP message, the testing mechanism extracts and records the relevant configuration parameters from the payload. When subsequent F1AP messages from the O-CU include related F1AP or RRC fields, the mechanism conducts consistency checks against the previously stored values. If any suspicious or inconsistent configurations are detected, the system promptly alerts the O-DU. If both the first and second stages pass validation, the process proceeds to the third stage.



(a) State machine of F1AP message (b) State machine of RRC message (C) State machine of NAS message

FIGURE 8. State Machine of Message

C. VERIFYING FAILURE CAUSE WITHIN THE NAS MESSAGES

In the third stage, the testing mechanism examines the NAS messages contained in the packets sent from the O-CU. These messages include fields that, according to standard protocol behavior, should be controlled exclusively by the AMF. The O-CU's unauthorized modification of these fields may disrupt the establishment of the NAS connection, necessitating independent validation of the message type and content. According to the FSM definition, if the NAS message in v_j belongs to the successful category, the message flow is valid and NAS-related services remain unaffected. Conversely, if the NAS message is categorized as unsuccessful, the system enters a NAS establishment failure state. Typical examples include *Registration Reject* and *Authentication Failure*. Since NAS-related field values in such messages are generally transmitted only once and lack redundancy, they cannot be cross-compared with other NAS messages from the O-CU. Therefore, upon detecting a NAS failure message, the testing mechanism analyzes the IEs within it to determine the cause of the failure.

These IEs contain critical indicators, such as the *5GMM cause*, which provides standardized failure codes including *Illegal UE*, *MAC failure*, and *ngKSI already in use*. These parameters are essential for diagnosing whether the O-CU may have improperly altered NAS-related fields via F1AP. Upon detecting such anomalies, the mechanism immediately warns the O-DU. The message is forwarded to the O-DU if the third stage is also successfully passed. Overall, using IEs enables the testing mechanism to validate the integrity of NAS-related fields within F1AP messages and prevent connection disruptions caused by protocol violations. Once all three stages are passed, the mechanism records the relevant settings for future cross-message consistency checks and allows the packet to proceed to the O-DU.

D. VALIDATION SCOPE AND FSM INDEPENDENCE

The proposed framework conducts conformance testing during the pre-deployment stage, where the O-DU evaluates the behavior of a vendor-supplied O-CU before admitting it into the operational network. According to 3GPP TS 38.401 [32], an O-DU connects to a single O-CU through one F1 association, while an O-CU may manage multiple O-DUs. Our testbed follows this topology and validates each candidate O-CU individually.

In the current experiment, one UE connects to the O-CU to demonstrate the verification process. When multiple UEs are involved, the framework assigns one FSM instance to each UE. Each FSM tracks its own F1AP signaling context, including the SCTP association and UE identifier. Because FSMs do not share global state, one UE's signaling never affects another. The processing cost grows linearly with the number of FSM instances, and the framework can distribute FSM execution across threads when necessary. By isolating UE contexts, the system avoids cross-flow false positives. False negatives arise only when optional 3GPP or O-RAN procedures are not included in the FSM; we reduce this risk by deriving all FSM rules directly from standardized message sequences. To handle future extensions to F1AP, the framework treats any unknown message as an unmodeled event and logs it for inspection, preventing false alarms caused by newly introduced procedures.

Based on this per-UE FSM design, the framework reports violations in line with its pre-deployment role. When an FSM

This article has been accepted for publication in IEEE Open Journal of the Communications Society. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJCOMS.2025.3649885

detects a rule violation, it immediately issues an alert that includes the violated rule, the affected UE context, and the corresponding F1AP/RRC/NAS message trace. Because the framework serves as a validation tool rather than a runtime enforcement system, it does not block message flows or isolate devices. These alerts serve as remediation triggers by providing the operator and vendor with actionable diagnostic information. After receiving an alert, the vendor can analyze the root cause and submit a corrected O-CU implementation. This validation–correction–revalidation workflow ensures that only fully compliant O-CU implementations are admitted into the production network and provides a practical remediation mechanism during the pre-deployment onboarding process.

We define each FSM manually based on the procedures and message flows specified in the 3GPP and O-RAN standards. Each FSM encodes valid signaling paths and parameter constraints, providing full transparency and control over state transitions. When new 3GPP or O-RAN releases modify signaling procedures, we update the corresponding FSM modules through the same derivation process, leaving other modules unchanged. The rule sets follow a modular structure, so revisions do not disrupt unrelated logic. We tag each FSM with its corresponding specification release and record this metadata alongside the validation logs to maintain traceability, and we preserve earlier FSM versions for backward compatibility. This version-controlled, modular update strategy keeps the framework aligned with evolving specifications while maintaining interpretability and readiness for future RIC-side integration.

IV. DESIGN OF ATTACK SIMULATION STRATEGIES

To emulate potential issues originating from an O-CU implementation, we introduce a Malicious Component between the O-CU and the O-DU on the F1 interface, as illustrated in Fig. 7. This component intercepts legitimate F1AP messages, mutates selected information elements, and forwards modified messages to the O-DU so that the resulting abnormal signaling appears to originate from the O-CU. These controlled abnormalities enable us to systematically evaluate the effectiveness of the conformance testing mechanism deployed at the O-DU.

Since pre-deployment conformance testing is the main focus of this work, vendor-side implementation flaws rather than external attacks are reflected in the injected abnormalities. When an O-CU mishandles cross-layer parameters, processes embedded signaling inconsistently, or departs from 3GPP-defined F1AP procedures, these weaknesses frequently occur in multi-vendor O-RAN deployments. Guided by the semantics of F1AP, RRC, and NAS procedures in the 3GPP specifications and informed by interoperability issues observed in heterogeneous O-CU implementations, we select three representative examples of abnormal behavior.

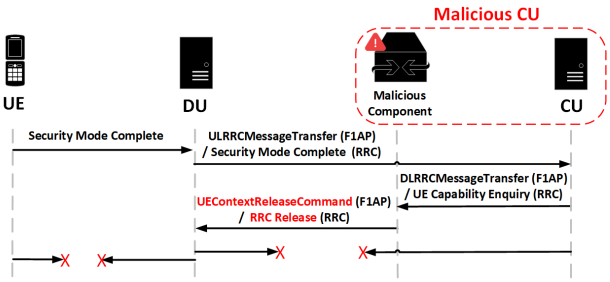


FIGURE 9. Scenario of unexpected F1AP message

A. INVALID SEQUENCE F1AP PACKETS

The first type of anomalous message involves an invalid sequence of F1AP packets. During the initial connection procedure between the UE and the RAN, F1AP signaling must follow a well-defined message sequence, as illustrated in Fig. 3. This procedure includes specific F1AP message types that must be transmitted in a strict and predefined order. If the O-CU transmits unexpected F1AP messages to the O-DU during this process, it may disrupt the RRC and NAS signaling flow or cause failure messages to be generated. In more severe cases, such abnormal sequences can cause the O-DU to malfunction or terminate its operations entirely.

To validate this error scenario, we injected a malicious intermediary component that modified the *DLRRCMessageTransfer* F1AP message sent from the O-CU to the O-DU, replacing it with an unrelated F1AP message. As shown in Fig. 9, the original *DLRRCMessageTransfer* message was replaced with a *UEContextReleaseCommand*. Once the O-DU received this anomalous F1AP message, it stopped communicating with the O-CU, which interrupted all subsequent F1AP procedures. This result shows that the injected abnormal message successfully terminated the ongoing F1AP signaling between the O-DU and O-CU and even prevented the establishment of the corresponding RRC connections. The underlying cause of this behavior is that the O-CU transmitted a message that violated the F1AP signaling sequence defined by the protocol specification.

B. F1AP MESSAGES WITH ANOMALOUS RRC PAYLOAD

The second type of anomalous message involves F1AP messages that contain malformed or tampered RRC payloads. As an example, we analyze the *Security Mode Command* RRC message encapsulated within the *DLRRCMessageTransfer* F1AP message. This message includes the *securityAlgorithmConfig* field, which specifies the cryptographic algorithms used for key exchange between the UE and the base station. The structure of this RRC payload is shown in Fig. 5. The O-CU configures the *securityAlgorithmConfig* field and sends it to the O-DU through the RRC message, after which the O-DU forwards it to the UE. If the UE determines that the encryption and integrity protection algorithms specified in the configuration match its supported capabilities, the subsequent RRC messages exchanged between the UE and

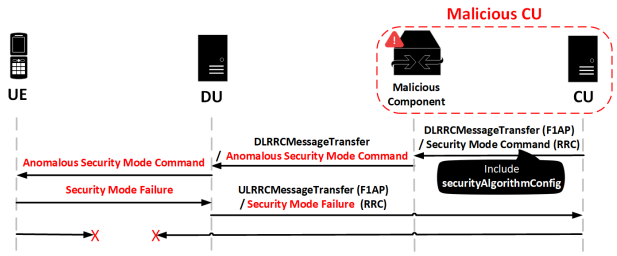


FIGURE 10. Scenario of anomalous RRC payload in F1AP message

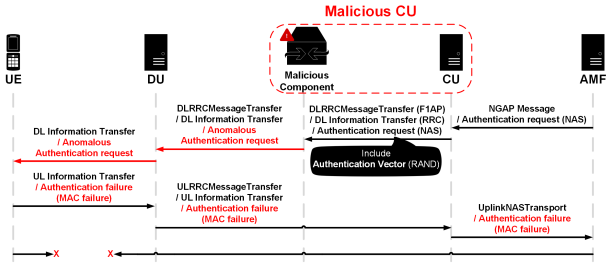


FIGURE 11. Scenario of anomalous NAS payload in F1AP message

the base station are protected using secure keys. In this case, the UE responds with a successful RRC message, *Security Mode Complete*, enabling the establishment of a secure NAS connection. However, if the algorithm configuration does not match the UE's supported capabilities, the UE returns an unsuccessful RRC message, *Security Mode Failure*. This response terminates the RRC connection and prevents the NAS from establishing a connection.

To verify this error scenario, we modified the integrity protection algorithm setting in the *securityAlgorithmConfig* field of the F1AP message using the malicious intermediary component, changing the value from IA2 to IA0. As shown in Fig. 10, after receiving the modified message, the O-DU returned the unsuccessful RRC message *Security Mode Failure*, indicating that the UE rejected the establishment of the RRC security connection with the O-CU. This result confirms that the manipulated algorithm setting successfully disrupted the expected security setup process. It is important to note that the *securityAlgorithmConfig* field is a parameter that the O-CU is legitimately authorized to configure in accordance with 3GPP specifications. However, if the O-CU assigns values that are incompatible with the UE's reported capabilities, such as specifying an unsupported integrity algorithm, this leads to a protocol-level inconsistency. While the message format and flow may appear syntactically valid, the content violates the logical constraints of the security negotiation procedure. Therefore, this type of misconfiguration underscores the importance of conformance testing in detecting errors that arise from incorrect yet superficially compliant signaling behavior.

C. F1AP MESSAGES WITH ANOMALOUS NAS PAYLOAD

The third type of anomalous message involves F1AP messages carrying abnormal NAS payloads. As an example of such an attack, we analyze the *Authentication Request* NAS message encapsulated within the F1AP message *DL-RRCMessageTransfer*. This message contains the Authentication Vectors (AVs), which the core network uses to authenticate the UE's identity during the NAS connection establishment procedure. The AV includes parameters such as *ABBA*, *RAND*, and *AUTN*, as illustrated in Fig. 6. Taking the *RAND* value as an example, it is generated by the AMF and transmitted to the O-CU via NAS signaling. The O-CU then forwards it to the O-DU, which subsequently delivers it to the UE. The UE uses its locally stored key to verify the validity of the received *RAND*. If the verification is successful, the UE returns an *Authentication Response* message to the AMF containing the verification result. Upon validating the response, the AMF proceeds with the NAS authentication procedure to confirm the UE's identity. However, if the UE receives an incorrect or tampered *RAND*, it detects the anomaly during MAC verification of the *Authentication Request* message. In such cases, the UE responds with an *Authentication Failure* message, thereby preventing the successful establishment of the NAS connection.

To verify this error scenario, we used a malicious intermediary component to modify the original *RAND* value in the F1AP message. As shown in Fig. 11, after the O-DU received and forwarded the modified message to the UE, the UE's authentication process failed. This resulted in the UE responding with an *Authentication Failure*, indicating that the manipulated *RAND* value successfully caused the UE to reject the establishment of a secure NAS connection. Since the NAS protocol is not primarily managed by the O-CU, the root cause of this anomaly lies in the unauthorized modification of a NAS field that, under regular protocol operation, should be set only by the AMF. This type of misbehavior highlights the importance of verifying the integrity of NAS-related fields within F1AP messages.

V. EVALUATION

The overall architecture is shown in Fig. 12. All experimental environments in this paper, including hardware specifications and software versions, are summarized in Table 1.

A. RESEARCH QUESTION

To assess whether the mechanism captures procedure-level and cross-layer inconsistencies rather than only syntax errors, we evaluate it against three representative examples of abnormal F1AP behavior and investigate the following research questions:

- **RQ1:** Can stateful FSM validation detect procedure-level violations in F1AP message sequencing?
- **RQ2:** Can cross-layer consistency checking identify mismatches between F1AP procedures and the embedded RRC messages?
- **RQ3:** Can NAS validation detect inconsistencies involving NAS parameters carried within F1AP messages?

TABLE 1. System Specifications and Software Versions

Category	Component	Specification
Host Computer	CPU	AMD Ryzen 9 9900X
	Memory	64GB
	OS	Windows 11 Education
Virtualization Platform	Hypervisor	VMware Workstation 17 Pro
Guest	vCPU	10
	Memory	16GB
	Disk	100GB
	OS	Ubuntu 20.04 LTS
Software Environment	5G gNB	OpenAirInterface (OAI)
	5G Core Network	OpenAirInterface (OAI)
	UE (Emulated)	OpenAirInterface (OAI)
	UE (Commercial)	Galaxy S20 5G
Software Defined Radio	Device	Ettus USRP B210

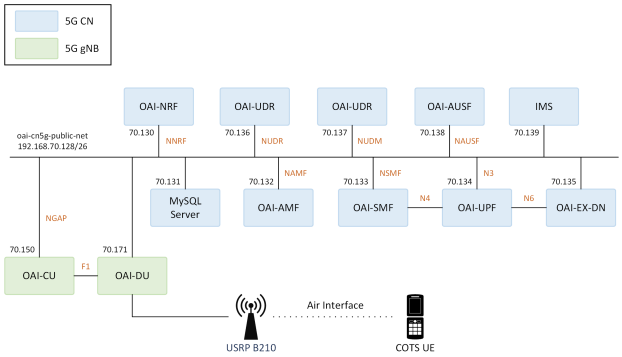


FIGURE 12. OpenAirInterface Architecture

Each research question is evaluated using a real O-CU implementation to demonstrate the coverage of our conformance mechanism and its advantages over generic fuzzing-based robustness testing.

1) INVALID SEQUENCE F1AP PACKETS

To address RQ1 and demonstrate that the conformance testing mechanism can detect malformed F1AP packets with invalid message sequences, we implemented the attack scenario as described in Section IV-A.

As shown in Fig. 13, the O-CU was initially expected to send the F1AP message *DLRRCMessageTransfer* to the O-DU. The preceding F1AP message exchanged between the O-CU and O-DU did not include any NAS message indicating a request to terminate NAS services. Therefore, according to the NAS FSM, the system was still operating under the assumption that the NAS service was in a stable connection state. However, the anomalous message type was

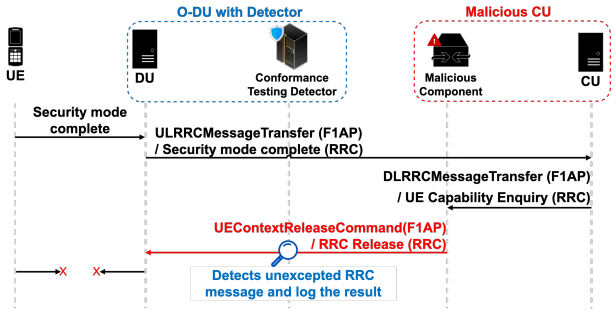


FIGURE 13. Detect unexpected F1AP message

modified to *UEContextReleaseCommand*, which requests immediate termination of the F1AP connection, and to *RRC Release*, which tears down the RRC connection. This violates the legitimate message path defined in the FSM, as the NAS connection should be terminated before releasing the F1AP and RRC connections. As a result, the FSM determines that the received F1AP and RRC messages are anomalous. The conformance testing mechanism records this violation, notifies the O-DU, and reports it to the user, indicating that the system has successfully identified an invalid sequence of F1AP messages.

2) F1AP MESSAGES WITH ANOMALOUS RRC PAYLOAD

To address RQ2 and demonstrate that the conformance testing mechanism can detect malicious RRC payloads encapsulated within F1AP packets sent by the O-CU, we implemented the attack scenario as described in Section IV-B.

Before the anomalous RRC message *Security Mode Command* is sent to the O-DU, a legitimate NAS message of the same name is first transmitted via an F1AP message from the O-CU to the O-DU. This NAS message contains the security algorithm capabilities supported by the UE. Upon receiving this legitimate NAS message, the conformance testing mechanism records the UE's current algorithm configuration—Ciphering: EA0, EA2; Integrity: IA2. Subsequently, the system receives the anomalous RRC message *Security Mode Command*. Since the message's procedural flow is valid, the mechanism proceeds to examine the *securityAlgorithmConfig* field in the RRC message, as shown in Fig. 14. If the integrity protection algorithm specified in *securityAlgorithmConfig* is set to IA0, which is inconsistent with the previously recorded UE capabilities, the conformance testing mechanism flags this inconsistency and issues a warning to the O-DU. This result confirms that the mechanism successfully detected the anomalous configuration in the RRC message payload.

3) F1AP MESSAGES WITH ANOMALOUS NAS PAYLOAD

To address RQ3 and demonstrate that the conformance testing mechanism can detect malicious NAS payloads en-

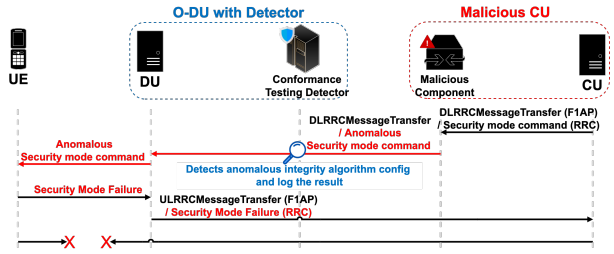


FIGURE 14. Detect F1AP message with Malformed RRC Payload

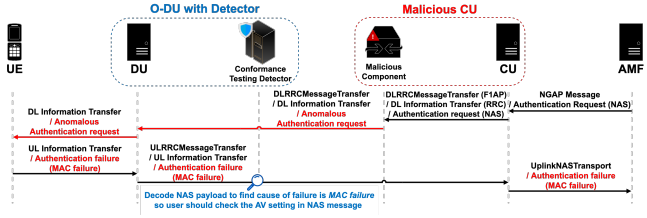


FIGURE 15. Detect F1AP message with Malformed NAS Payload

capsulated within F1AP packets sent by the O-CU, we implemented an attack scenario, as described in Section IV-C.

The cause of the anomalous NAS message payload scenario described earlier lies in the O-CU injecting a manipulated AV value—specifically, an abnormal *RAND* value—into the F1AP message, which subsequently causes the UE to respond with an *Authentication Failure*. Since the AV must be verified either by the UE or by the AMF, it isn't easy to directly detect such anomalies at the O-DU side by simply deconstructing the AV content in the F1AP message. However, we observed that by monitoring the subsequent NAS messages sent from the O-CU to the O-DU, the detection mechanism can still identify abnormal NAS connection behavior and raise appropriate alerts.

When the FSM within the detection mechanism observes an *Authentication Failure* message returned by the UE, it classifies the event as a failed NAS connection. Since the message follows a valid procedural flow, the detection mechanism proceeds to analyze the NAS message's payload. By parsing the IEs in the *Authentication Failure* message, the mechanism determines that the failure is due to a *MAC Failure*. This indicates a problem in the previously received *Authentication Request* message and suggests that the O-CU may have illegitimately altered a NAS payload field. The detection mechanism subsequently issues a warning to the O-DU about the abnormal NAS message configuration, thereby demonstrating that the anomaly has been successfully identified.

B. EFFICIENCY ANALYSIS

In our 5G O-RAN environment, we conducted a comparative analysis of scenarios with and without a conformance testing mechanism, specifically examining differences in connection times across various F1AP service stages. Throughout

TABLE 2. Latency evaluation with and without testing

Procedure	With testing (ms)		Without testing (ms)	
	Mean	Std. Dev.	Mean	Std. Dev.
F1 Setup	0.518	0.096	0.555	0.118
RRC Setup	23.541	6.766	18.975	2.557
NAS Setup	89.948	8.294	85.827	4.904
F1 UE Context Setup	0.663	0.320	0.619	0.243
F1 UE Context Release	5.974	1.707	3.626	0.983
Summation	**120.644**	**13.153**	**109.603**	**5.950**

the experiment, we captured packets using Wireshark. For each environment, we collected 100 sets of packets and categorized them by their respective F1AP service stage. We then computed the connection time for each category. To reduce the impact of outliers, we calculated the average processing time based on the 100 packets in each category. The statistical results of the packet processing times are summarized in Table 2.

According to Table 2, deploying the conformance testing mechanism increases the connection-processing time across different F1AP service phases by approximately 10–20%. The largest latency gap occurs in the *RRC Setup* and *NAS Setup* stages, where the average processing time increases from 18.975 ms to 23.541 ms and from 85.827 ms to 89.948 ms, respectively. The corresponding standard deviations (6.766 ms and 8.294 ms) remain moderate, indicating stable timing behavior across repeated trials, for lightweight signaling procedures such as *F1 Setup*, *UE Context Setup*, and *UE Context Release*, the latency difference remains below 3 ms. Overall, the total connection time increases from 109.603 ms (without testing) to 120.644 ms (with testing), representing an approximate 10% rise. This increase primarily results from the behavior of the SCTP protocol, which underlies F1AP transmission. When message inspection during testing introduces brief processing delays, SCTP may retransmit identical payloads, producing redundant packets and slightly extending total transmission time. Despite this additional delay, the end-to-end connection latency of 120.64 ms remains well below the 150 ms control-plane limit defined for 5G systems. These results confirm that the proposed conformance testing mechanism adds only minimal overhead while maintaining interface stability and deterministic timing behavior. More importantly, the current design enables the O-DU to perform pre-deployment consistency checks on O-CU components from third-party vendors, ensuring protocol compliance and operational reliability before network integration.

VI. CONCLUSION

This paper presents a conformance testing mechanism for the F1 interface in the O-RAN architecture, designed to detect abnormal behavior from potentially non-compliant or malicious O-CU components. Built on the OAI platform,

our system introduces a malicious intermediary to simulate forged F1AP messages, which are then validated by a detection module deployed at the O-DU. The proposed mechanism parses message types and field-level information, verifies signaling sequences using the FSM, and evaluates critical security parameters, such as encryption algorithm settings. Experimental results demonstrate that the mechanism can effectively identify malformed F1AP messages, protocol violations, and security misconfigurations across the RRC and NAS layers. It also provides real-time alerts to the O-DU with detailed diagnostics. Notably, the mechanism operates passively and does not interfere with the actual F1 interface traffic, making it suitable for integration into production environments. The proposed approach offers extensibility and can be further enhanced through integration with RIC components in the O-RAN ecosystem to support intelligent, policy-driven protocol validation. Future work will focus on optimizing system performance for large-scale deployment, extending coverage to additional O-RAN interfaces, and enabling the validator to export violation reports to the SMO or the Near-RT RIC, so operators can automate onboarding decisions or quarantine non-compliant O-CU implementations when necessary.

REFERENCES

[1] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE communications surveys & tutorials*, vol. 18, no. 3, pp. 1617–1655, Feb 2016, doi: https://doi.org/10.1109/COMST.2016.2532458.

[2] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 2, pp. 1376–1411, Jan. 2023, doi: https://doi.org/10.1109/COMST.2023.3239220.

[3] A. S. Abdalla, P. S. Upadhyaya, V. K. Shah, and V. Marojevic, "Toward next generation open radio access networks: What O-RAN can and cannot do!" *IEEE Netw.*, vol. 36, no. 6, pp. 206–213, Nov./Dec. 2022, doi: https://doi.org/10.1109/MNET.108.2100659.

[4] O-RAN ALLIANCE Working Group 11, "O-RAN Security Threat Modeling and Risk Assessment 3.0," O-RAN ALLIANCE," Technical Specification, 2024.

[5] R. Gangula, A. Lacava, M. Polese, S. D'Oro, L. Bonati, F. Kaltenberger, P. Johari, and T. Melodia, "Listen-while-talking: Toward dapp-based real-time spectrum sharing in O-RAN," *arXiv preprint arXiv:2407.05027*, Jul 2024, doi: https://doi.org/10.48550/arXiv.2407.05027.

[6] Y. Huang, Q. Sun, N. Li, Z. Chen, J. Huang, H. Ding, and C.-L. I, "Validation of current O-RAN technologies and insights on the future evolution," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 2, pp. 487–505, Nov 2023, doi: https://doi.org/10.1109/JSAC.2023.3336180.

[7] Y.-X. Lin, B.-K. Hong, and S.-M. Cheng, "Conformance testing for 5G O-RAN entities through MEC," in *IEEE 2022 CANDARW*, Himeji, Japan, Nov 2022, doi: https://doi.org/10.1109/CANDARW57323.2022.00070.

[8] 3GPP TS 38.472, "NG-RAN; F1 signalling transport," 3GPP," Technical Specification, Apr. 2024.

[9] 3GPP TS 33.501, "Security architecture and procedures for 5G System," 3GPP," Technical Specification, Mar. 2024.

[10] 3GPP TS 38.473, "NG-RAN; F1 Application Protocol (F1AP)," 3GPP," Technical Specification, Mar. 2024.

[11] O-RAN ALLIANCE Working Group 1, "O-RAN architecture description 12.0," O-RAN ALLIANCE," Technical Specification, June 2024. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications

[12] M. Kouchaki, A. S. Abdalla, and V. Marojevic, "OpenAI dApp: An Open AI platform for distributed federated reinforcement learning apps in O-RAN," in *Proc. 2023 IEEE FNWF*, Baltimore, MD, USA, Nov. 2023, pp. 1–6, doi: https://doi.org/10.1109/FNWF58287.2023.10520642.

[13] P. S. Upadhyaya, N. Tripathi, J. Gaeddert, and J. H. Reed, "Open AI Cellular (OAIC): An open source 5G O-RAN testbed for design and testing of AI-Based ran management algorithms," *IEEE Network*, vol. 37, no. 5, pp. 7–15, Sept. 2023, doi: https://doi.org/10.1109/MNET.2023.3320933.

[14] 3GPP TS 38.470, "NG-RAN; F1 general aspects and principles," 3GPP," Technical Specification, Mar. 2024.

[15] 3GPP TS 38.471, "NG-RAN; F1 layer 1," 3GPP," Technical Specification, Apr. 2024.

[16] S. Sullivan, A. Brighente, S. A. Kumar, and M. Conti, "5G security challenges and solutions: a review by OSI layers," *IEEE Access*, vol. 9, pp. 116 294–116 314, Aug 2021, doi: https://doi.org/10.1109/ACCESS.2021.3105396.

[17] O-RAN ALLIANCE Working Group 11, "O-RAN Study on Certificate Management Framework 2.0," O-RAN ALLIANCE," Technical Specification, 2024.

[18] S. J. Seelam, S. Andra, and P. C. Jain, "Impact of remote radio head on 5G Open-RAN technology," in *Proc. IEEE 2022 ICSC*, Noida, India, Dec 2022, doi: https://doi.org/10.1109/ICSC56524.2022.10009237.

[19] O-RAN ALLIANCE Working Group 7, "O-RAN deployment scenarios and base station classes 4.0," O-RAN ALLIANCE," Technical Specification, Oct. 2022.

[20] D. Mimran, R. Bitton, Y. Kfir, E. Klevansky, O. Brodt, H. Lehmann, Y. Elovici, and A. Shabtai, "Security of open radio access networks," *Comput Secur*, vol. 122, p. 102890, Nov. 2022, doi: https://doi.org/10.1016/j.cose.2022.102890.

[21] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN security: Challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 214, p. 103621, May 2023, doi: https://doi.org/10.1016/j.jnca.2023.103621.

[22] J. Groen, S. D'Oro, U. Demir, L. Bonati, M. Polese, T. Melodia, and K. Chowdhury, "Implementing and evaluating security in O-RAN: Interfaces, intelligence, and platforms," *IEEE Network*, pp. 1–1, July 2024, doi: https://doi.org/10.1109/MNET.2024.3434419.

[23] S. Soltani, M. Shojafar, A. Brighente, M. Conti, and R. Tafazolli, "Poisoning bearer context migration in O-RAN 5G network," *IEEE Wireless Commun. Lett.*, vol. 12, no. 3, pp. 401–405, Dec. 2023, doi: https://doi.org/10.1109/LWC.2022.3227676.

[24] 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. NDSS 2024*, San Diego, California, Feb 2024, doi: https://doi.org/10.14722/ndss.2024.24527.

[25] Z. A. E. Houda, H. Moudoud, and B. Brik, "Federated deep reinforcement learning for efficient jamming attack mitigation in O-RAN," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 7, pp. 9334–9343, Jan 2024, doi: https://doi.org/10.1109/TVT.2024.3359998.

[26] N. Makris, C. Zarafetas, P. Basaras, T. Korakis, N. Nikaein, and L. Tassiulas, "Cloud-based convergence of heterogeneous RANs in 5G disaggregated architectures," in *Proc. IEEE 2018 ICC*, Kansas City, MO, USA, May 2018, doi: https://doi.org/10.1109/ICC.2018.8422227.

[27] J. Groen, S. D'Oro, U. Demir, L. Bonati, D. Villa, M. Polese, T. Melodia, and K. Chowdhury, "Securing O-RAN open interfaces," *IEEE Trans. Mobile Comput.*, pp. 1–13, Apr. 2024, doi: https://doi.org/10.1109/TMC.2024.3393430.

[28] O-RAN ALLIANCE Working Group 11, "O-RAN Security Test Specifications 7.0," O-RAN ALLIANCE," Technical Specification, 2024.

[29] O-RAN ALLIANCE Test & Integration Focus Group, "O-RAN End-to-end Test Specification 6.0," O-RAN ALLIANCE," Technical Specification, 2024.

[30] 3GPP TS 38.331, "NR; Radio Resource Control (RRC); Protocol specification," 3GPP," Technical Specification, Apr. 2024.

[31] 3GPP TS 24.501, "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 ," 3GPP," Technical Specification, Apr. 2024.

[32] 3GPP TS 38.401, "NG-RAN; Architecture description," 3GPP," Technical Specification, Mar. 2024.

[33] 3GPP TS 33.511, "Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class," 3GPP," Technical Specification, Mar. 2024.

[34] 3GPP TS 33.523, "5G Security Assurance Specification (SCAS); Split gNB product classes," 3GPP," Technical Specification, Mar. 2024.
[35] 3GPP TS 33.840, "Study on security aspects of the disaggregated gNB architecture," 3GPP," Technical Specification, Dec. 2020.
[36] C.-F. Hung, Y.-R. Chen, C.-H. Tseng, and S.-M. Cheng, "Security threats to xApps access control and E2 interface in O-RAN," *IEEE Open J. Commun. Society*, vol. 5, pp. 1197–1203, Feb. 2024, doi: https://doi.org/10.1109/OJCOMS.2024.3364840.
[37] K. Thimmaraju, A. Shaik, S. Flück, P. J. F. Mora, C. Werling, and J.-P. Seifert, "Security testing the O-RAN Near-Real Time RIC & A1 interface," in *Proc. 17th ACM WiSEC*, New York, USA, Feb. 2024, p. 277–287, doi:https://doi.org/10.1145/3643833.3656118.
[38] 3GPP TS 33.523, "5G security assurance specification (SCAS)," 3GPP," Technical Specification, July 2025.
[39] 3GPP TS 33.117, "Catalogue of general security assurance requirements," 3GPP," Technical Specification, June 2025.

CHENG-FENG HUNG (Member, IEEE) received the M.E. degree in information technology and applications from the College of Science and Engineering at the National Quemoy University, Kinmen, Taiwan, in 2019, and the Ph.D. degree in computer science and information engineering from the National Taiwan University of Science and Technology, Taipei, in 2025. He is currently a Fixed Term Researcher with the Cybersecurity Research Institute, National Institute of Information and Communications Technology, Tokyo, Japan. His research focuses on O-RAN and AI security.

SHIH-SHIUNG CHANG received the B.S. and M.S. degrees in computer science and information engineering from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2021 and 2024, respectively. He received the Best Paper Award in CISC 2020 and the Best Student Paper Award in CISC 2024. He joined some projects with the Institute for Information Industry and Trend Micro. He served as the speaker in NQUSIC. His current research interests are LTE and O-RAN security in mobile networks and web security.

TSUNG-YEN HSIEH received the B.S. degree in computer science and information engineering from Tamkang University, Taiwan, in 2024. He is currently pursuing the M.S. degree in computer science and information engineering at the National Taiwan University of Science and Technology, Taiwan. His research interest is O-RAN security in mobile networks.

SHIN-MING CHENG (Member, IEEE) received his B.S. and Ph.D. degrees in computer science and information engineering from National Taiwan University, Taipei, Taiwan, in 2000 and 2007, respectively. Since 2012, he has been on the faculty of the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei, where he is currently a professor. He served as the Deputy Director-General in Administration of Cyber Security, Ministry of Digital Affairs, from 2022 to 2025 and as the Acting Director-General in 2025. His current interests are mobile network security, IoT system security, malware analysis and AI robustness. He has received IEEE Trustcom 2020 Best Paper Awards.

TAO BAN (Member, IEEE) received his B.E. degree from Xi'an Jiaotong University in 1999, M.E. degree from Tsinghua University in 2003, and Ph.D. degree from Kobe University in 2006, respectively. He is currently a chief senior researcher with Cybersecurity Research Institute, National Institute of Information and Communications Technology, Tokyo, Japan. His research interest includes network security, malware analysis, machine learning, and data mining.

TAKESHI TAKAHASHI (Senior Member, IEEE) is the Director General of the Center for Research on AI Security and Technology Evolution at Japan's National Institute of Information and Communications Technology, where he leads a research team focused on AI and cybersecurity. He holds a Ph.D. in telecommunications from Waseda University. Prior to joining NICT in 2009, he held positions as a researcher at Tampere University of Technology, a JSPS Research Fellow at Waseda University, and a business consultant at Roland Berger Ltd.While at NICT, he also served as a visiting research scholar at the University of California, Santa Barbara (2019–2020), and as a management trainee at the Cabinet Office of Japan (2021–2022).