Computing&AI Connect
ISSN: 3104-4719
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx
OPEN ACCESS
SCIFINITI PUBLISHING
Research Article

Security Assurance for 5G Split gNB and AMF Vulnerabilities

Yi-Hsueh Tsai,[1] Shiang-Jiun Chen✉,[2]

[1] National Taipei University of Technology, Taipei, 10608, Taiwan
[2] Institute for Information Industry, Taipei 105412, Taiwan;

ORCID IDs:

https://orcid.org/0009-0007-9676-9365

https://orcid.org/0009-0002-7542-2374

Abstract

As 5G networks continue to evolve and innovate, security challenges are emerging, necessitating a more rigorous assessment of their security mechanisms, particularly within core functions such as the Access and Mobility Function (AMF) and disaggregated gNodeB (gNB). 5G's virtualized architecture represents a significant increase in complexity compared to pre-4G network architectures, and its software-based architecture necessitates enhanced security. This study examines security issues within protocol design, device integration, and virtualized infrastructure, drawing on 3GPP specifications and security vulnerabilities observed in early 5G deployments. By examining the effectiveness of fundamental security measures such as encryption, integrity protection, and replay prevention, we also conduct a comprehensive and systematic assessment of 5G deployments in terms of resilience. To enhance security, this paper also explores the anomaly detection and adaptive response capabilities of automated and AI-driven threat detection systems, as well as how to enhance real-time monitoring. The goal is to address these technical vulnerabilities and practical implementation challenges systematically. The main purpose of this research is to enhance the security of 5G networks and ensure they can withstand increasingly sophisticated cyber threats.

Keywords

5G core network security; User Plane Function (UPF); Distributed Denial of Service (DDoS); fuzz, AMF vulnerabilities

SCIFINITI PUBLISHING

Introduction

5G provides faster data transmission speeds and lower response times through high-frequency millimeter waves, focused signal beams, and advanced antenna systems. These technologies enable industrial applications that rely on real-time communication, such as smart factories and self-driving car networks. In addition to faster transmission speeds, 5G's ultra-reliable low-latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC) [1] features also change innovative applications in fields such as medicine, automobiles, and smart manufacturing.

The core architecture of 5G is software-driven, combining virtualization, cloud technology, and network slicing to provide customized services with Quality of Service (QoS) for different application requirements. However, virtualization structures and network slicing also increase security risks and expose new vulnerabilities, so stronger protection measures are needed. Unlike traditional networks, 5G networks are developed based on software definition. Its network softwareization and function virtualization (NFV) [2] characteristics each may bring potential vulnerabilities, so more rigorous security measures are urgently needed.

One of the characteristics of 5G is its ability to connect millions of devices. However, Internet of Things (IoT) devices have limited computing resources, and their security features are insufficiently protected [3]. Coupled with the risk of cross-slice attacks that may occur in network slices and vulnerabilities in software-driven infrastructure, it is necessary to establish a comprehensive security framework. This paper explores the multifaceted security challenges and conducts a detailed analysis of the security of 5G core components, including gNodeB (gNB), Access and Mobility Management Function (AMF), User Plane Function (UPF), and Session Management Function (SMF). It also focuses on how to enhance the resilience of 5G networks against emerging threats by referencing 3GPP technical specifications to ensure the establishment of a secure, reliable, and innovative communications ecosystem [4-6].

Related Work on 5G Security Vulnerabilities

With the widespread adoption of 5G networks, their security vulnerabilities have become more important. 5G security issues include multiple aspects: protocol vulnerabilities, attack surfaces, and mitigation strategies. This section summarizes the main findings and identifies key areas where security measures require strengthening.

Protocol vulnerabilities

Recent 3GPP standards (including TS 33.501 [7] and TS 33.512 [5] based on 3GPP standards) have pointed out that 5G's NAS and RRC protocols have multiple vulnerabilities. NAS replay attacks can exploit unsynchronized sequence numbers, allowing attackers to resend expired authentication requests to gain unauthorized access. Meanwhile, RRC downgrade attacks exploit unencrypted signaling exchanges to force the connection to downgrade to a less secure mode.

To address these issues, stronger encryption mechanisms and stricter sequence number checks can be introduced at the access layer (AS) to effectively reduce the risks. These vulnerabilities affect network reliability and allow attackers to manipulate communication processes. Experts emphasize the need to address these challenges through robust encryption mechanisms, data integrity protection, and unique identification of data packets.

Replay attacks, in which attackers retransmit intercepted messages to deceive network entities, thereby subverting authentication and session management processes. Strict sequence number checks and timestamp verification ensure message timeliness and legitimacy, mitigating related risks. Furthermore, advanced encryption technologies and AI-driven anomaly detection can enhance threat identification and response capabilities in real time. Strengthening the security of NAS and RRC protocols can effectively maintain the confidentiality, integrity, and availability of 5G networks and effectively defend against growing cyber threats.

Man-in-the-Middle (MitM) Attacks

Man-in-the-middle (MitM) attacks pose a serious threat to 5G networks, especially in the unprotected F1-C and N2 signaling channels. Research results show that attackers can use malicious base stations to intercept control plane messages and tamper with authentication and key exchange procedures. Vulnerabilities in the EAP-AKA authentication mechanism can be exploited due to weak integrity verification [8], allowing adversaries to inject forged security mode commands. To address these vulnerabilities, enforcing end-to-end encryption at the NGAP layer and periodically renegotiating session keys are key measures to limit the risk of interception. Standard defenses such as secure key exchange and integrity checks have been widely adopted [9]. In addition, emerging approaches such as quantum key distribution (QKD) are being investigated further to strengthen the security resilience of 5G networks.

Distributed Denial of Service (DDoS) Attacks

Distributed denial-of-service (DDoS) attacks [10-11] can disrupt 5G services on a large scale, significantly impacting 5G information security. Mitigating such threats typically involves using anomaly detection systems or rate limiting. Common approaches include using artificial intelligence (AI) and machine learning (ML) to analyze and identify traffic patterns to detect and prevent malicious activity.

Network Slicing Vulnerabilities

The flexibility of network slicing also presents security risks. Network slicing security can be achieved through slice isolation or other methods to prevent cross-slice attacks [12-13], including access control policies and real-time monitoring of slice-specific traffic. These measures ensure that a compromise of one slice does not compromise the security of other slices.

Internet of Things and Device-Level Security

Internet of Things (IoT) device vulnerabilities [14-15], particularly in 5G network environments, have become a significant security issue. Common issues include weak authentication mechanisms, a lack of encryption, and the use of outdated firmware. Proposed solutions to improve IoT security include secure boot processes, firmware integrity checks, and device-level encryption protocols. Distributed Denial-of-Service (DDoS) attacks [10-11] are a focal point of security research due to their potential to disrupt 5G services on a large scale. Research emphasizes the importance of anomaly detection systems and rate-limiting mechanisms for mitigating these threats. Leveraging artificial intelligence and machine learning for traffic analysis and pattern recognition has emerged as a promising real-time strategy for detecting and preventing malicious activities.

Methods

Mitigation Strategies

The architectural complexity and diverse functionalities of 5G networks introduce several security vulnerabilities that require tailored countermeasures. This section comprehensively analyzes the most critical vulnerabilities and their corresponding mitigation strategies, emphasizing the importance of proactive approaches to ensure network integrity and reliability. The vulnerability identification process leverages a systematic methodology that combines targeted protocol analysis with automated testing to detect weaknesses in 5G network functions. For example, replay attacks are detected by using tools that monitor for repeated or out-of-sequence messages, and then analyze sequence number mismatches in NAS and RRC signaling. MitM threats could be identified by employing protocol analyzers to detect anomalies in encryption or integrity checks, and then inspecting unauthorized key exchanges or data interception attempts across interfaces. DDoS risks are assessed by simulating high-volume traffic floods and monitoring network performance degradation, with AI-driven anomaly detection systems identifying irregular patterns. These identification processes are integrated into the testing framework, enabling precise mitigation strategies, such as robust encryption algorithms, dynamic key management, and real-time traffic monitoring.

Protocol Weaknesses

Vulnerabilities in signaling protocols such as Non-Access Stratum (NAS) and Radio Resource Control (RRC), as defined in 3GPP TS 33.501 (Release 18) and 3GPP TS 33.512 (Release 18), render them susceptible to attacks like replay and downgrade [16-18]. Without adequate encryption and integrity protection, attackers can manipulate these protocols to disrupt communications or downgrade security settings to weaker 4G or 3G protocols. To address this issue, mitigation measures include implementing robust encryption algorithms, such as AES-256 for NAS signaling as specified in 3GPP TS 33.501, and ensuring integrity protection through HMAC-SHA-256 for all signaling data. replay prevention mechanisms incorporate unique sequence identifiers and timestamp-based validation, as mandated by 3GPP TS 33.512, to detect and block repeated messages. To ensure compliance and robustness, these standards-based countermeasures are tested within the SCAS framework and with specific test cases validating encryption strength and sequence number integrity under simulated attack scenarios.

To strengthen these countermeasures, the proposed framework integrates AES-256-GCM encryption for NAS signaling and HMAC-SHA-256 integrity protection for all control-plane messages. Replay prevention is enforced through unique sequence identifiers combined with timestamp-based validation, in line with 3GPP TS 33.512 specifications. In addition, dynamic key refresh mechanisms are applied at

session establishment and within predefined time intervals to minimize exposure to key compromise. These cryptographic safeguards are validated within the SCAS framework using simulated replay and downgrade attacks, with performance evaluated through metrics such as latency overhead, detection accuracy, and false positive rates in anomaly detection.

Man-in-the-Middle (MitM) Threats

Man-in-the-middle (MitM) attacks pose a significant threat to network security by intercepting or manipulating communications between 5G components. The distributed architecture of 5G networks increases the opportunities for attackers to position themselves within the communication path, particularly across interfaces like F1, N2, and N3, as outlined in 3GPP TS 33.523 (Release 18). Mitigation strategies encompass end-to-end encryption using Transport Layer Security (TLS) 1.3 for N2 interface communications, secure key exchange mechanisms based on Diffie-Hellman protocols, and periodic data integrity verification through cryptographic checksums, as recommended by 3GPP TS 33.501. Emerging technologies, such as Public Key Infrastructure (PKI) and Zero Trust frameworks, further enhance resilience against MitM attacks by enforcing mutual authentication and continuous verification, ensuring robust protection across diverse 5G network scenarios [19].

Distributed Denial of Service (DDoS) Risks

The scalability of 5G networks introduces a higher risk of DDoS attacks, which can overwhelm network resources and disrupt services. Common attack vectors include flooding signaling pathways or exploiting compromised IoT devices. Effective countermeasures include employing rate limiting, traffic filtering, and AI-driven anomaly detection systems to identify and block malicious traffic patterns in real time.

IoT Device Vulnerabilities

Integrating IoT devices into 5G networks has introduced new entry points for attackers. Many IoT devices lack proper authentication, encryption, and firmware updates, making them vulnerable to exploitation. Recommended mitigations include secure boot processes, periodic firmware validation, and enforcing device-level security standards. Additionally, network segmentation can isolate compromised devices to prevent lateral movement of attacks.

Network Slicing Isolation Challenges

While network slicing offers flexibility by creating virtual networks tailored to specific use cases, it also introduces risks of cross-slice attacks if isolation is not adequately enforced. An attacker accessing one slice can exploit shared resources to compromise others. Mitigation strategies include robust slice isolation mechanisms, continuous traffic monitoring, and dynamic access control policies to safeguard slice-specific data and functionalities [20].

Software Vulnerabilities in Virtualized Environments

5G networks are based on SDN and NFV architectures, which introduce software vulnerabilities. Attackers can exploit flaws in the hypervisor, API, or orchestration system to compromise network integrity. Risk mitigation can include regular vulnerability assessments, timely software patching, secure configuration management, and hypervisor hardening [21-22].

Enhanced Security Framework for Optimization of 5G Security Assurance for gNB-CU Testing

The gNB is a critical element in 5G networks, serving as the intermediary between User Equipment (UE) and the 5G core network. Its role is particularly crucial in the context of 5G's advanced capabilities, such as network slicing, URLLC, and mMTC. Given these functionalities, ensuring the security of the gNB, particularly its Central Unit (gNB-CU), is essential [23-26].

The gNB-CU manages control and user plane operations, rendering it a high-value target for potential cyber threats. To mitigate these risks, several key security mechanisms have been developed. These encompass robust authentication protocols, encryption techniques, and integrity checks to prevent replay attacks, data tampering, and unauthorized access. Furthermore, advanced anomaly detection systems are employed to identify and respond to suspicious activities in real time.

To keep the gNB-CU (a key part of 5G networks) secure, several testing methods are used to check for various types of attacks. These tests evaluate how well the encryption algorithms work, ensure the robustness of signaling integrity and reliability, and confirm the gNB-CU can hold up under simulated cyber-attacks. Using machine learning machine

learning models to spot and predict unusual activity also boosts security, helping to stop threats before they cause harm.

Moreover, secure software development is a big focus. This includes regularly reviewing code and checking for weaknesses in the gNB-CU software. Regular updates and patches fix any newly found issues, keeping the gNB-CU system protected against evolving threats.

Together, these security steps and testing methods strengthen the gNB-CU, making sure it meets the tough, demanding requirements of 5G networks while staying secure. They protect user data and network operations and ensure everything lines up with regulatory standards and industry best practices [23-26].

The solution enhances the SCAS testing process by streamlining UE registration to cover multiple test cases in a single session, minimizing resource consumption and latency. The test environment leverages a virtualized 5G network setup, simulating critical network functions such as the gNB-CU, gNB-, compliant with TS 33.523 standards. Key test parameters include signaling protocols such as Stream Control Transmission Protocol (SCTP) for F1 interface communications, F1 Application Protocol (F1AP) for gNB-DU-to-gNB-CU signaling, as specified in 3GPP TS 33.501. These protocols are tested under simulated attack scenarios, including replay attacks (detected via sequence number mismatches), MitM attacks that are monitored through unauthorized key exchanges, and DDoS attacks, which are assessed via traffic flooding.

Replay and Tampering Protection for gNB-CUs

Replay attacks and data tampering pose serious threats to the integrity and reliability of the gNB-CUs in 5G networks. To rigorously evaluate their mitigation capabilities, this study employed a structured methodology consisting of four steps: (1) UE Registration and Security Establishment: The UE initiates the RRC Setup and Security Mode procedures, which establish a secure channel using the Authentication and Key Agreement (AKA) protocol defined in 3GPP TS 33.501.[7] (2) Replay Injection: This attack simulates adversary behavior by retransmitting previously valid messages (such as Security Mode Complete) or uplink data with incorrect MAC values. Replay detection mechanisms combine timestamp verification with secure nonce generation to ensure that retransmitted packets are rejected. (3) Tampering Detection and Integrity Verification: Packet authenticity is ensured through techniques such as cryptographic hashing and digital signatures. Abnormal or replayed messages are detected and discarded at both the RRC and PDCP layers. (4) Secure Session Continuation: Only authenticated packets are allowed to proceed with PDU session establishment and secure uplink/downlink data exchange. End-to-end encryption and session-based key management further ensure confidentiality and integrity between the gNB-CU and the UE.

This replay and tamper protection framework demonstrates how to implement the integrity protection conditions defined by 3GPP, combining timestamp verification, cryptographic authentication, and dynamic session key management to effectively mitigate the risk of replay and tampering threats throughout the communication process [26-28].

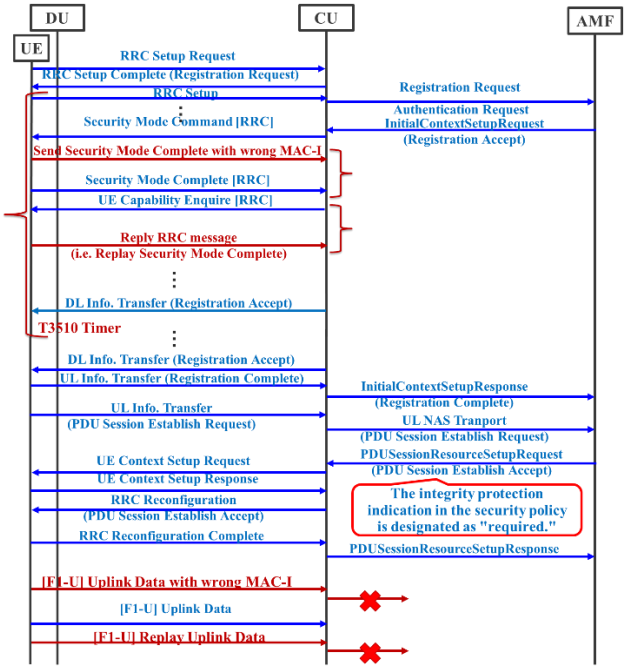

Figure 1: Workflow of Replay and Tamper Protection Tests

Figure 1 shows Sequential flow of replay and tamper protection testing in the 5G core network. Blue arrows indicate normal signaling from UE registration to session establishment; red arrows indicate malicious replay behavior (e.g., retransmitting a Security Mode Complete message with an incorrect MAC-I). Integrity check failures at the RRC and PDCP layers are marked with a red X, indicating that the packet is rejected. Only messages that pass verification can proceed to complete secure session establishment,

fully demonstrating the implementation of the integrity protection strategy in 3GPP TS 33.501.

Multi-SCAS Testing with Single-UE Connections

Conventional SCAS (Security Assurance Specification) testing for gNB-CU often employs isolated test cases that lead to prolonged testing times and substantial resource utilization. This approach proposes integrating multiple SCAS test scenarios within a single UE session, thereby enhancing the efficiency of the testing process. By leveraging dynamic session management techniques, the framework reduces redundancy in signaling exchanges and optimizes network resource allocation.

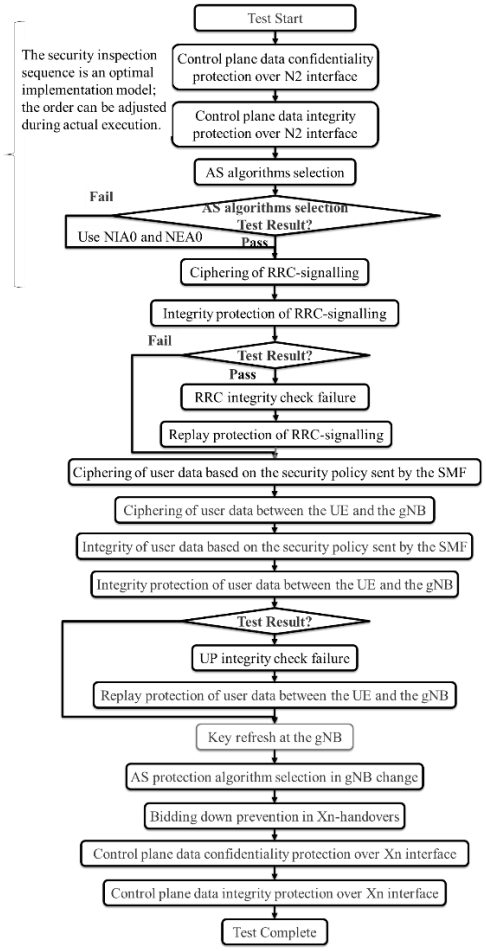

Figure 2: Process Flow for Single-UE Multi-SCAS Testing

In particular, the method utilizes layered signaling protocols that allow concurrent validation of security parameters across various network functions such as gNB, AMF, and SMF. This multi-faceted approach not only accelerates the overall testing cycle but also ensures comprehensive coverage of potential security vulnerabilities. Figure 2 highlights these concurrent testing interactions, demonstrating the streamlined flow of signaling messages between UE, AMF, and gNB, which facilitates effective detection of anomalies and ensures robust network security postures.

Additionally, the architecture supports seamless transition between test scenarios without necessitating session reinitialization, thus minimizing overhead and enhancing throughput. This unified approach enhances the reliability of 5G network security evaluations by providing real-time insights into the performance of multiple components under diverse conditions.

Interface Security: F1, N2, and N3 Protections

The gNB-CU communicates through multiple interfaces, each presenting distinct security challenges and requiring robust protection mechanisms.

1. F1 Interface: Responsible for communication between the gNB-CU and gNB-DU, this interface is particularly vulnerable to integrity attacks targeting radio signals. Encryption protocols and integrity checks are implemented to secure signaling data transmission and counter such threats.

2. N2 Interface: Handling control plane communication between the gNB-CU and the core network, this interface demands stringent confidentiality measures. Advanced encryption standards protect control plane data from unauthorized access and tampering.

3. N3 Interface: Facilitating user plane data transmission, the N3 interface is secured through comprehensive data protection strategies, including encryption and traffic isolation, ensuring user data remains secure during transit.

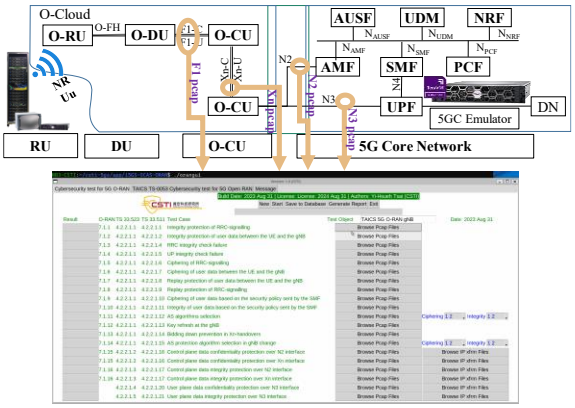

Figure 3: Interface Layer Protections and Security Test Workflow

The gNB-CU communicates through multiple interfaces, each presenting distinct security challenges and requiring robust protection mechanisms. Figure 3 provides a clear diagram of the security validation processes for the F1, N2, and N3 interfaces, detailing how encryption standards, integrity checks, and isolation methods are applied. This workflow-organized approach ensures each interface is secured properly, meeting strict security standards and boosting the overall strength of the 5G network infrastructure.

Security Mechanisms: Integrity, Ciphering, and Replay Prevention

To keep Radio Resource Control (RRC) signaling and user plane data transmission secure, strong integrity protection mechanisms are essential. This includes using advanced encryption algorithms to keep data private and dynamic key management protocols to block unauthorized access. The system also incorporates integrity checks to confirm that the data is authentic and hasn't been tampered with during transmission. Additionally, to prevent replay attacks, where hackers try to reuse intercepted data, sequence number checks are put in place to stop this kind of exploitation. Several testing procedures are done to make sure the encryption holds up against interception, unauthorized decryption, and replay attacks, creating a secure and reliable communication environment [26].

SCAS Automation for Fault Detection

Automation significantly enhances Security Assurance Specifications (SCAS) testing by efficiently detecting unresponsive elements within the gNB-CU environment. The system employs automated scripts and real-time monitoring tools to continuously scan network components, promptly identifying anomalies such as inactive nodes, protocol failures, and unexpected latencies. This proactive monitoring generates immediate alerts, enabling swift intervention and minimizing service disruptions. Automated error-handling routines further ensure that detected faults are logged, analyzed, and resolved without manual intervention, thereby maintaining continuous security validation and operational integrity [26]. The flowchart illustrates the detection and response mechanisms for non-responsive elements, including initial connectivity checks, heartbeat signal verification, and automated error correction processes [26] (see Figure 4).

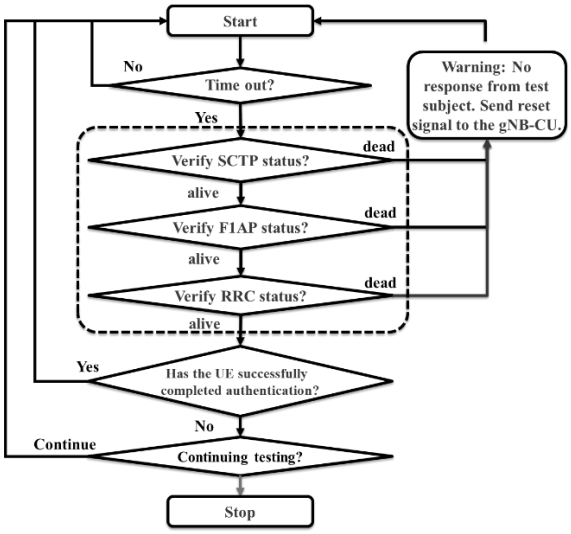

Figure 4: Non-Responsive Device Detection Flow

Stepwise SCAS Testing Implementation

A systematic and layered approach to SCAS testing ensures a comprehensive security assessment of the gNB-CU across various operational phases. The process begins with UE (User Equipment) authentication, verifying device legitimacy through mutual authentication protocols and secure key exchanges. Subsequent phases involve rigorous testing of the control plane, user plane, and transport layers, ensuring each is robust against potential threats [26].

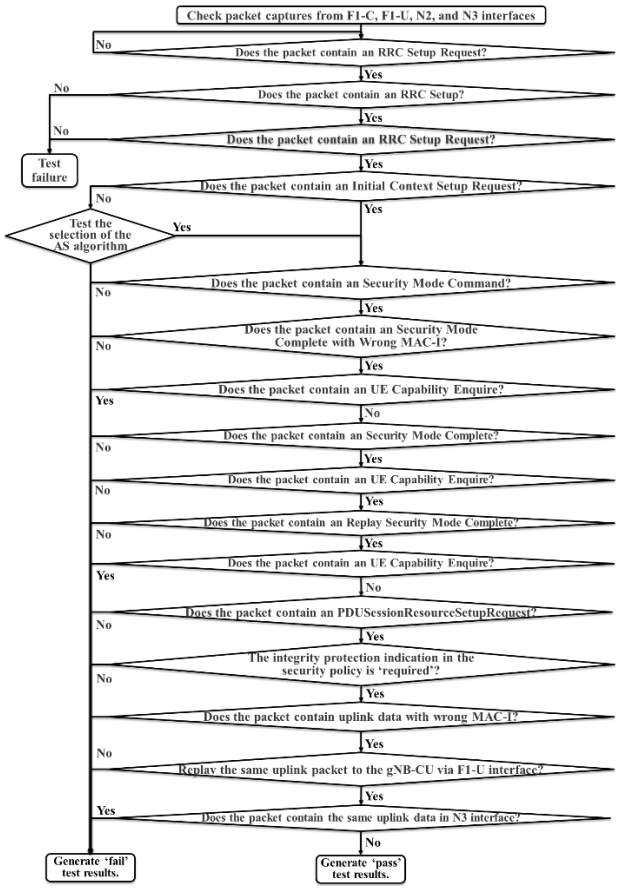

Figure 5: SCAS Testing Workflow for gNB-CU
Each testing cycle is followed by automated resets and state re-initializations, ensuring the system is consistently prepared for subsequent test iterations, thus preventing cumulative errors [26].

Figure 5 presents the SCAS testing workflow, outlining the sequence from connection setup and execution of predefined test cases to iterative reset mechanisms that facilitate continuous validation and fault isolation [26].

Optimization of 5G Security Assurance for AMF Testing

The Access and Mobility Management Function (AMF) is critical in 5G networks, handling user authentication, mobility management, and session integrity. Ensuring robust security assurance for the AMF within the Security Assurance Specification (SCAS) framework is essential, but the process is often resource-intensive and prone to redundancy. Traditional testing approaches frequently involve repeated User Equipment (UE) connection attempts for each security parameter, leading to significant inefficiencies and increased operational complexity.

To address these challenges, optimizing AMF testing workflows is imperative for maintaining high security standards while improving efficiency. Key challenges include:

1. High Resource Consumption: Traditional SCAS methods necessitate repetitive connection attempts for individual test items, resulting in excessive network load and resource wastage. This inefficiency is further exacerbated by the need to maintain secure communication channels during each iteration.

2. Testing Redundancy: Repeated sessions for validating similar security attributes introduce unnecessary overhead, slowing down the testing process and consuming additional resources without proportional benefits.

3. Limited Real-Time Adaptation: Conventional methods often lack mechanisms for efficiently detecting non-responsive elements during testing, leading to delays in fault identification and resolution. Implementing adaptive testing mechanisms that can dynamically adjust based on network responses can mitigate this issue.

Using intelligent mechanisms, smart tools like automated session grouping and anomaly-based error detection can significantly improve the efficiency of testing the Access and Mobility Management Function (AMF). By employing machine learning algorithms to spot patterns and predict issues, testing can adapt on the fly, cutting down on unnecessary steps while still ensuring thorough security validation. Additionally, using state-aware testing setups can save resource consumption by keeping session details consistent across multiple tests, avoiding the need to repeatedly set up connections. repeated connection overheads.

Furthermore, using virtualization techniques to simulate complex 5G environments allows for in-depth, thorough security assessments without needing a ton of physical equipment, thus saving both money and resources.. These improvements not only make AMF testing processes smoother but also strengthen the overall security of 5G networks by enabling faster detection and fixing of potential weaknesses..

Enhanced SCAS Testing Mechanism

An intelligent automated Security Assurance Specification (SCAS) testing system is proposed to tackle the complexity and heavy resource demands of SCAS testing in 5G networks. Unlike prior SCAS

testing approaches, this work introduces a novel single-UE multi-SCAS testing framework, enabling concurrent validations with reduced overhead. This new approach combines multiple test cases into fewer sessions, making the testing processes much smoother while still fully covering security requirements defined in 3GPP specifications, TS 33.512, which specifies the use of sequence number validation and timestamp-based verification for detecting repeated NAS messages. The methodology is structured into two primary components:

1. Single-UE Connection for Multi-SCAS Testing: A single-user equipment (UE) registration instance is leveraged to validate multiple SCAS test cases simultaneously. This methodology reduces connection overhead, optimizes resource utilization, and accelerates testing workflows by minimizing repeated authentication and registration cycles. The system dynamically manages session contexts, ensuring a single UE can sequentially execute diverse SCAS test scenarios without reinitialization. In order to enhance practical applicability, the testing framework incorporates scenarios, such as simulated man-in-the-middle (MitM) attacks on the N2 interface, and replay attacks on NAS signaling. These scenarios are designed to mimic realistic network conditions, ensuring robust security testing of 5G network functions like the AMF and gNB-CU under diverse attack vectors. The system significantly expands scenario coverage by supporting up to 10 concurrent SCAS test cases per UE session, covering vulnerabilities across the control plane, user plane, and transport layers.

2. Automated Non-Responsive Element Detection: The framework includes continuous real-time monitoring of the Access and Mobility Management Function (AMF) responses. Automated recovery procedures mitigate faults like signaling failures or session drops, validated through protocols such as SCTP, NAS, and NGAP. This mechanism reduces manual intervention and ensures operational reliability, as illustrated in Figure 6. It detects non-responsive elements promptly and mitigates faults through automated recovery procedures. This proactive mechanism enhances reliability by reducing manual intervention and swiftly addressing faults such as signaling failures, session drops, or delayed authentication. To ensure comprehensive fault detection in operational environments, our practical testing scenarios include simulated network outages and protocol failures, validated through real-time monitoring of SCTP, NAS, and NGAP protocols.

The attached flow diagram (Figure 7) illustrates the process flow [29], showcasing how a single UE connection efficiently manages multiple SCAS test cases concurrently. It details the signaling interactions with core network components, including the AMF, Authentication Server Function (AUSF), and gNodeB (gNB), demonstrating the streamlined signaling flow and optimized session handling under realistic network conditions. This enhanced mechanism ensures that 5G core security testing is more efficient, less resource-intensive, and highly reliable.

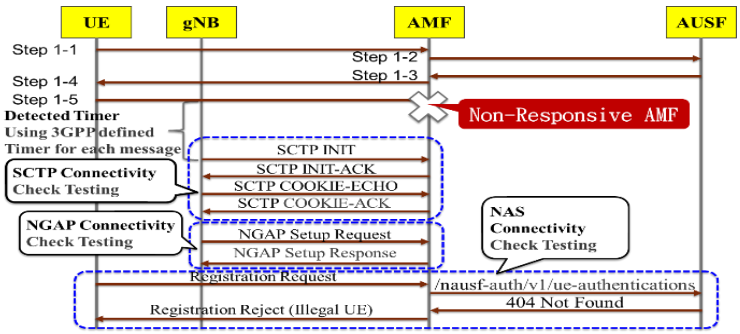

Figure 6: Non-Responsive AMF Detection Process

Implementation Details and Technical Solutions

The proposed framework is organized into a clear step-by-step process. SCAS requirements are first defined following 3GPP TS 33.512, and a single-UE testbed is established using NFV-based AMF, gNB, AUSF, and SMF functions. Multi-SCAS scenarios are then executed within one UE session to minimize overhead, with continuous monitoring of latency, resource utilization, and test coverage. Finally, validation against anomaly and fault detection rules ensures reliable identification of replay, MitM, and non-responsive elements under realistic conditions. This solution enhances the SCAS testing process by streamlining UE registration to cover multiple test cases in a single session. This optimization reduces the need for repetitive registration steps, minimizing resource consumption and latency. The test environment leverages a 5G network setup, simulating critical network functions such as the AMF, gNB, AUSF, and SMF using network function virtualization (NFV) platforms, compliant with 3GPP TS 33.512 standards. Key test parameters include signaling protocols such as Stream Control Transmis-

sion Protocol (SCTP) for N2 interface communications, Non-Access Stratum (NAS) for UE-AMF interactions, and Next Generation Application Protocol (NGAP) for gNB-AMF signaling.

Each test sequence is meticulously synchronized with AMF, UE, AUSF, and gNB signaling exchanges, ensuring precise validation and efficient execution [29-30]. The unified data analysis provides comprehensive insights into security performance by processing aggregate test outputs across diverse scenarios and enabling scalability for large-scale deployments. Specific metrics evaluated include latency reduction in session setup time and test case concurrency levels, such as up to 10 simultaneous SCAS test cases per UE session. The proposed SCAS testing framework streamlines UE registration to cover multiple test cases in a single session, minimizing resource consumption and latency. The methodology follows a structured, step-by-step process::

1. Network Access Initiation: The UE sends an initial access request to the AMF, triggering the testing framework, as shown in Figure 7.

2. Concurrent Execution of SCAS Test Cases: Multiple test cases run simultaneously, each validated through defined signaling interactions involving SCTP, NAS, and NGAP protocols, reducing overall test time by eliminate repeated testing procedure.

3. Unified Data Analysis: Test outputs are aggregated for comprehensive analysis, allowing for holistic assessment of security parameters and streamlined reporting, as depicted in Figure 6 for non-responsive device detection.

The scalable framework is validated across different network functions such as AMF, gNB, AUSF, SMF and deployment scenarios. Figure 7 illustrates the signaling flow for concurrent test case execution, while Figure 6 details the automated detection and alert mechanism for non-responsive elements, ensuring alignment with the described methodology.

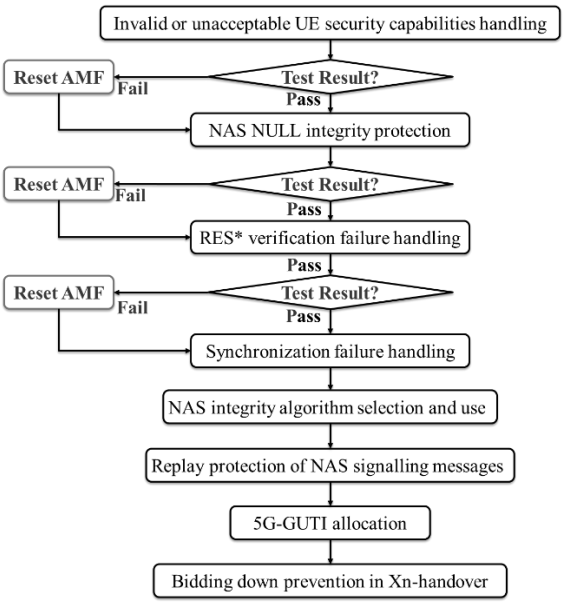

Figure 7: Process Flow for Single-UE Multi-SCAS Testing

A vital enhancement is the automated detection mechanism for non-responsive devices during SCAS testing [29]. This mechanism continuously monitors device responsiveness across protocols such as SCTP, NAS, and NGAP, facilitating early identification of faults as shown in Figure 8. This process includes:

1. Connectivity Checks: Initiating checks across essential protocols to ensure continuous device responsiveness.

2. Fault Logging: Documenting faults when devices fail to respond within defined thresholds.

3. Automated Alerts: Notifying operators promptly, enabling swift troubleshooting and minimizing downtime.

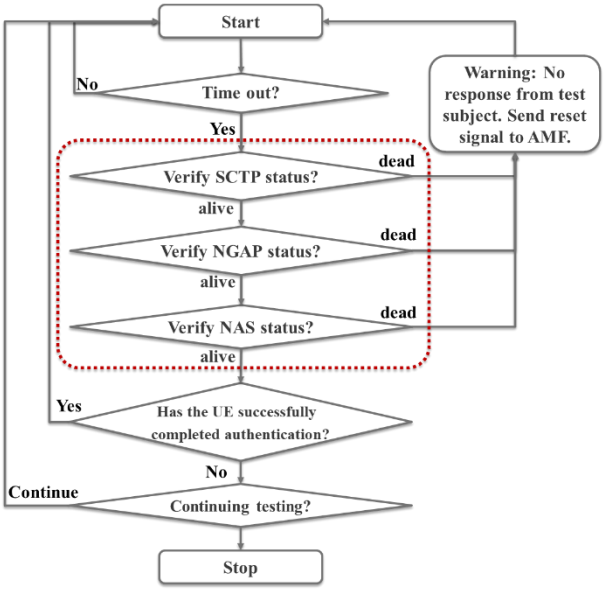

Figure 8: Non-Responsive Device Detection Flow

The detection and alert flow are visually represented to illustrate the sequence of monitoring, fault detection, logging, and alerting, ensuring seamless management of non-responsive devices. Figure 6 visualizes the detection and alert flow, showing each step involved in monitoring connectivity and handling non-responses, including the automated logging and alert mechanisms.

Results

The optimized SCAS testing framework improves AMF efficiency by eliminating redundant operations and incorporating automation for real-time fault detection and resolution [29]. This ensures that 5G networks remain resilient against emerging threats without resource strain. Future improvements could integrate AI-driven adaptive testing mechanisms for dynamic and personalized security assessments, enhancing network protection through continuous learning and automated adjustments. While the main contribution of this work lies in the design and implementation of the proposed testing framework, we also outline an evaluation methodology to guide subsequent validation. The planned assessment covers end-to-end latency, CPU and memory utilization, test coverage, and fault detection accuracy under single-UE multi-SCAS scenarios. Although full-scale experimental results are beyond the current scope, these defined metrics establish a clear roadmap for comprehensive validation in our extended research.

Discussions and Conclusions

This study proposed a single-UE multi-SCAS testing framework and an automated fault detection mechanism to demonstrate how original design innovations can enhance testing efficiency, reduce latency, and improve anomaly detection accuracy, and also highlights the vulnerabilities inherent in 5G's architecture, particularly in key components like the Access and Mobility Management Function (AMF) and split gNodeB (gNB) product classes. The research underscores the critical need for robust security mechanisms through a detailed analysis of protocol weaknesses, device-level risks, and virtualization vulnerabilities.

Robust encryption, replay attack prevention, network slicing isolation, and real-time threat detection are critical measures for securing the 5G infrastructure. Integrating these technologies with standardized testing frameworks, including proactive patch management, enables a more effective response to evolving security threats. Beyond technical enhancements, collaboration among regulatory bodies, network operators, and technology providers can further strengthen 5G security.

Regarding future work and methodological improvements, which include further enhancing the proposed SCAS testing framework, future work will focus on integrating AI-driven adaptive testing mechanisms to enable dynamic and personalized security assessments. These mechanisms will leverage machine learning algorithms to predict and prioritize test cases based on real-time network conditions, improving fault detection accuracy and reducing testing overhead.

Additionally, to support 6G network architectures, we will expand the framework, including advanced network slicing and ultra-low-latency scenarios, and ensure scalability for next-generation networks. Methodological improvements for SCAS testing will include the development of standardized performance benchmarks, such as latency and throughput, to facilitate cross-vendor comparisons. These advancements aim to ensure continuous learning and adaptation, strengthening the security assurance process for future 6G networks.

List of abbreviations

5G: Fifth Generation Mobile Network
AMF: Access and Mobility Management Function
gNB: gNodeB (Next-Generation Node B)

SCAS: Security Assurance Specification
URLLC: Ultra-Reliable Low-Latency Communications
eMBB: Enhanced Mobile Broadband
mMTC: Massive Machine-Type Communications
NFV: Network Function Virtualization
SDN: Software-Defined Networking
IoT: Internet of Things
PKI: Public Key Infrastructure

Author Contributions

Conceptualization and supervision, Y.-H. Tsai S.-J. Chen; methodology, S.-J.Chen.; validation, Y.-H. Tsai;, formal analysis, S.-J.C.;, investigation Y.-H. Tsai and S.-J. Chen; resources, Y.-H. Tsai and S.-J. Chen;, data curation, Y.-H. Tsai and S.-J. Chen;, writing - original draft preparation, Y.-H. Tsai and S.-J. Chen;, writing - review and editing, Y.-H. Tsai and S.-J. Chen;, project administration, Y.-H. Tsai and S.-J. Chen. Figures 5, 7, and 8 by S.-J. Chen all other figures by Y.-H. Tsai. All authors have read and agreed to the published version of the manuscript.

Availability of Data and Materials

All data supporting the findings are included in the manuscript.

Consent for Publication

Not applicable.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

No external funding was received for this research.

Acknowledgments

The authors used an AI-based text checking tool solely for language editing and proofreading purposes. No content generation was performed by AI.

References

[1] A. Pradhan, S. Das, M. J. Piran, and Z. Han, "A survey on security of ultra/hyper reliable low latency communication: Recent advancements, challenges, and future directions," arXiv, vol. 2404.08160v1, Apr. 2024. [Online]. Available: https://arxiv.org/abs/2404.08160

[2] S.-J. Chen, T.-Y. Wang, C.-S. Fang, and I.-W. Chiang, "Security Assessment of Low Earth Orbit (LEO) with Software-Defined Networking (SDN) Structure," 2023 IEEE 6th International Conference on Knowledge Innovation and Invention (ICKII), Sapporo, Japan, 2023, pp. 620–624, doi: 10.1109/ICKII58656.2023.10332792.

[3] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 2015, pp. 336–341, doi: 10.1109/ICITST.2015.7412116.

[4] J. Mongay Batalla, et al., "Multi-layer security assurance of the 5G automotive system based on multi-criteria decision making," IEEE Trans. Intell. Transp. Syst., vol. 99, no. 1, 2023. [Online]. Available: https://doi.org/10.1109/TITS.2023.3325908

[5] 3GPP TS 33.512, "5G security assurance specification (SCAS); Access and Mobility Management Function (AMF)," Release 18.

[6] 3GPP TS 33.523, "5G security assurance specification (SCAS); split gNB product classes," Release 18.

[7] ETSI, *ETSI TS 133 501 V15.2.0 (2018-10): 5G; Security Architecture and Procedures for 5G System (3GPP TS 33.501 version 15.2.0 Release 15)*, European Telecommunications Standards Institute, 2018.

[8] J. Yang, S. Arya, and Y. Wang, "Formal-guided fuzz testing: Targeting security assurance from specification to implementation for 5G and beyond," IEEE Access, vol. 12, pp. 29175-29193, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3369613

[9] A. Qasem and A. Tahat, "Machine learning-based detection of the man-in-the-middle attack in the physical layer of 5G networks," Simul. Model. Pract. Theory, vol. 136, no. 2, p. 102998, 2024. [Online]. Available: https://doi.org/10.1016/j.simpat.2024.102998

[10] P. Benlloch-Caballero, Q. Wang, and J. M. Alcaraz Calero, "Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks," Comput. Netw., vol. 222, p. 109526, 2023. [Online]. Available: https://doi.org/10.1016/j.comnet.2022.109526

[11] A. Pagadala and G. Ahmed, "Analysis of DDoS attacks in 5G networks," in Proc. 14th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT), Delhi, India, 2023, pp. 1-6. [Online]. Available: https://doi.org/10.1109/ICCCNT56998.2023.10307311

[12] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices," arXiv, vol. 1901.01443, 2019. [Online]. Available: https://doi.org/10.48550/arXiv.1901.01443

[13] S. Wong, B. Han, and H. D. Schotten, "5G network slice isolation," arXiv, vol. 2203.01590v1, 2022. [Online]. Available: https://arxiv.org/abs/2203.01590

[14] A. Sousa and M. Reis, "5G security features, vulnerabilities, threats, and data protection in IoT and mobile devices: A systematic review," Evol. Stud. Imaginative Cult., 2024. [Online]. Available: https://doi.org/10.70082/esiculture.vi.1054

[15] M. Ryan and K. Y. Rozier, "A survey and analysis of recent IoT device vulnerabilities," Mar. 2024. [Online]. Available: https://doi.org/10.21203/rs.3.rs-3982790/v1

[16] D. Segura, J. Munilla, E. J. Khatib, and R. Barco, "5G early data transmission (Rel-16): Security review and open issues," IEEE Access, vol. 10, pp. 12345-12356, 2022. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3203722

[17] S. Eleftherakis, D. Giustiniano, and N. Kourtellis, "SoK: Evaluating 5G protocols against legacy and emerging privacy and security attacks," arXiv, vol. 2409.06360v1, 2024. [Online]. Available: https://arxiv.org/abs/2409.06360

[18] Y. Dong, R. Behnia, A. A. Yavuz, and S. R. Hussain, "Securing 5G bootstrapping: A two-layer IBS authentication protocol," arXiv, vol. 2502.04915v1, 2025. [Online]. Available: https://arxiv.org/abs/2502.04915

[19] A. A. Alquwayzani and A. A. Albuali, "A systematic literature review of zero trust architecture for military UAV security systems," IEEE Access, vol. 12, pp. 176033-56, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3503587

[20] M. Alicherry and A. D. Keromytis, "DoubleCheck: Multi-path verification against man-in-the-middle attacks," Dept. Comput. Sci., Columbia Univ., New York, NY, USA.

[21] X. Li, M. Samaka, H. A. Chan, and R. Jain, "Network slicing for 5G: Challenges and opportunities," IEEE Internet Comput., vol. PP, no. 99, pp. 1-1, 2018. [Online]. Available: https://doi.org/10.1109/MIC.2018.326150452

[22] A. Alnaim, "Securing 5G virtual networks: A critical analysis of SDN, NFV, and network slicing security," Int. J. Inf. Secur., vol. 23, no. 6, pp. 3569-3589, 2024. [Online]. Available: https://doi.org/10.1007/s10207-024-00900-5

[23] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," IEEE Commun. Surveys & Tutorials, vol. 25, no. 2, Second Quarter, 2023.

[24] W. Azariah et al., "A survey on open radio access networks: Challenges, research directions, and open source approaches," *Sensors*, vol. 24, no. 3, p. 1038, 2024. [Online]. Available: https://doi.org/10.3390/s24031038

[25] N. Raksasook, "Enhancing security in O-RAN through secure software development lifecycle analysis: A comprehensive study," M.S. thesis, Nat. Taipei Univ. Technol., Taipei, Taiwan, 2024.

[26] Y.-H. Tsai, "Information security testing method and information security testing system of open radio access network base station," U.S. Patent 12,107,881 B2, Oct. 1, 2024. [Online]. Available: United States Patent and Trademark Office (USPTO)

[27] M. Mahyoub et al., "Security analysis of critical 5G interfaces," TechRxiv, 2023. [Online]. Available: https://doi.org/10.36227/techrxiv.24069600

[28] GSM Association, "5G security guide," Version 3.0, FS.40 - Official Document, 2024. [Online]. Available: https://www.gsma.com

[29] Y.-H. Tsai, "Method for testing core network function entity, testing device and non-transitory computer-readable medium," U.S. Patent 12,088,485 B2, Sep. 10, 2024. [Online]. Available: United States Patent and Trademark Office (USPTO).

[30] GSM Association, "NESAS security assurance specification development guidelines," Version 1.0, FS.50 - Official Document, 2023. [Online]. Available: https://www.gsma.com