

Soft Tester UE: A Novel Approach for Open RAN Security Testing

Joshua Moore, Aly S. Abdalla, Charles Ueltschey and Vuk Marojevic
 Department of Electrical and Computer Engineering, Mississippi State University, USA
 {jjm702,asa298,cmu32,vm602}@msstate.edu

Abstract—With the rise of 5G and open radio access networks (O-RAN), there is a growing demand for customizable experimental platforms dedicated to security testing, as existing testbeds do not prioritize this area. Traditional, hardware-dependent testing methods pose challenges for smaller companies and research institutions. The growing wireless threat landscape highlights the critical need for proactive security testing, as 5G and O-RAN deployments are appealing targets for cybercriminals. To address these challenges, this article introduces the Soft Tester UE (soft T-UE), a software-defined test equipment designed to evaluate the security of 5G and O-RAN deployments via the Uu air interface between the user equipment (UE) and the network. The outcome is to deliver a free, open-source, and expandable test instrument to address the need for both standardized and customizable automated security testing. By extending beyond traditional security metrics, the soft T-UE promotes the development of new security measures and enhances the capability to anticipate and mitigate potential security breaches. The tool's automated testing capabilities are demonstrated through a scenario where the Radio Access Network (RAN) under test is evaluated when it receives fuzzer data when initiating a connection with an UE.

Index Terms—5G Security, O-RAN Security, Software-Defined, Open Source, O-RAN Testbeds, Automated Testing, Custom Procedures

I. INTRODUCTION

The rapid evolution of 5G and open radio access networks (O-RAN) necessitates the development of robust and flexible security testing mechanisms. Despite the increasing availability of 5G testbeds and research tools, customizable experimental platforms that can satisfy diverse requirements are still needed. Traditional testing approaches characterized by high costs associated with proprietary hardware and closed-source frameworks, present significant barriers towards achieving comprehensive security testing. Moreover, the dynamic wireless threat landscape, marked by sophisticated cyber threats targeting 5G and O-RAN deployments, underscores the necessity for proactive and advanced security testing techniques.

Open RAN architectures, with their disaggregated structure and open interfaces facilitating multi-vendor interoperability, introduce numerous vulnerabilities that make them prime targets for security attacks [1]. These vulnerabilities include potential exploits at different architecture components, ranging from the radio access network to the core network. To address these challenges, advanced security testing tools capable of assessing authentication mechanisms, encryption protocols, and the resilience of disaggregated network components under various attack scenarios are required.

Currently, security testing tools are limited within the literature. For example, tools like the A1 interface testing tool in [2] and those focused on Denial of Service (DoS) attacks on fronthaul interfaces in [3] and [4] are tailored to specific functionalities. However, much of the existing literature focused on testing operates in an ad-hoc manner, focusing on achieving stand-alone testing objectives rather than conducting comprehensive security assessments across the entire O-RAN ecosystem. An AI testing framework, as demonstrated in [5], exemplifies a comprehensive approach to testing but is focused on evaluating AI models within O-RAN deployments and does not consider security tests. In contrast, the framework proposed in [6] offers extensive customization of telemetry and code execution within O-RAN architectural components. However, it lacks built-in security testing capabilities and necessitates architectural modifications.

To address these challenges, this article introduces the Soft Tester UE (soft T-UE), a software-defined testing solution designed for evaluating the security posture of 5G and O-RAN deployments. This open-source tool, compatible with commercial-off-the-shelf (COTS) software radio hardware, empowers users to conduct standardized and customized security tests. The soft T-UE aims to serve as an expandable testing platform equipped with sample test cases, comprehensive documentation, automated CI/CD pipelines, performance benchmarks, configuration files, hardware setup guidelines, testing scripts, and comprehensive data collection capabilities for a wide range of testing scenarios. By advancing beyond traditional security metrics, the soft T-UE endeavors to foster the development of innovative security measures and enhance the ability to anticipate and mitigate potential security breaches in 5G and O-RAN environments. These efforts will culminate in a versatile testing tool capable of evaluating authentication mechanisms, encryption protocols, communication security, logging and monitoring systems, and network component resilience under various attack scenarios.

The structure of this paper unfolds as follows: Section II presents the system architecture and design of the soft T-UE. Section III details the testing methods and associated procedures. Section IV delves into implementation specifics and discusses the results obtained. Finally, the paper concludes by examining the potential impact of the soft T-UE on advancing 5G and O-RAN security testing methodologies.

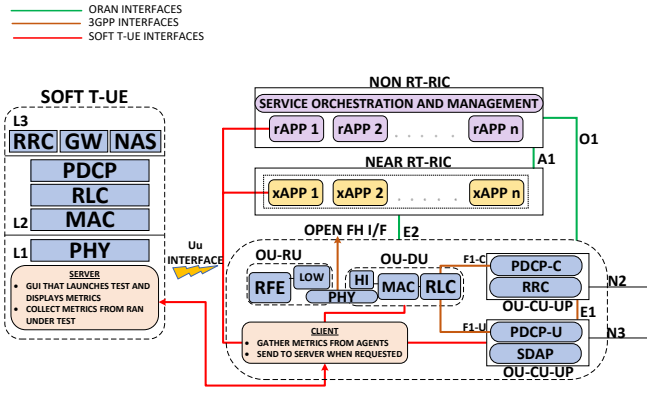


Fig. 1: Soft-T UE Architecture

II. SYSTEM ARCHITECTURE AND DESIGN

The architecture of the soft T-UE is engineered to enable rigorous testing of 5G and O-RAN security vulnerabilities without modification to the existing RAN architecture. Built upon srsRAN’s User Equipment (UE) structure, it modifies UE functionalities, messages, and signaling mechanisms to conduct precise tests on the RAN components and security procedures under examination. The soft T-UE is designed with modular architecture, allowing for easy integration of new features and capabilities. The modular approach enables the extension of the functionality of the soft T-UE through new test scenarios, metrics, and analysis tools without disrupting the core architecture. This flexibility is crucial for enabling the rapid integration of new tests to keep pace with the evolving threat landscape of 5G and O-RAN and the rapid development of O-RAN specifications and test requirements. Figure 1 shows the soft-T UE’s architecture from a high-level perspective showing the new interfaces provided, the components used to facilitate data gathering, and the visualization of live metrics.

The soft T-UE connects to the Radio Access Network (RAN) under test by probing the network and sending test vectors that represent different security tests or attacks. The connection establishment protocol in the soft T-UE follows the general 5G/Open RAN attach and connection establishment procedures. This includes initial access procedures, random access, Radio Resource Control (RRC) connection setup, security mode setup, authentication, and NAS procedures. The security mode setup ensures encryption and integrity protection before completing authentication and NAS procedures, such as attach requests and PDU session establishments. The RAN’s responses to these vectors are logged, providing valuable data for both black box and white box RANs. Through soft T-UE, we can introduce a modified version of the regular UE exchanged packets with the RAN during the connection establishment phase or even after this while evaluating the various default security metrics or even defining new metrics and collecting data during each test for a comprehensive test environment. This data-centric approach allows for a thorough understanding of the RAN’s resilience to various types of attacks. The components of the soft T-UE’s architecture include:

- **UE Functionality:** The soft T-UE functions as a standard

UE, with additional capabilities for launching security tests. It supports 4G LTE, 5G NSA, and SA configurations, and can operate in black box, white box, and test configurations. The soft T-UE leverages the existing srsRAN UE architecture, ensuring compatibility with commercial off-the-shelf software radio hardware.

- **Logging and Data Collection:** The soft T-UE architecture features robust logging and data collection mechanisms essential for a comprehensive assessment of the RAN’s performance and security. Central to this setup is a client-server model facilitating communication between the RAN under test and the soft T-UE. The client component accepts asynchronous connections from multiple agents concurrently, enabling simultaneous testing of multiple components within each attack scenario. This approach enhances testing scalability and operational efficiency across varied RAN environments. The server component manages incoming data streams, logging real-time UE status, operational parameters, and key performance indicators (KPIs) in JSON format.
- **Graphical User Interface (GUI):** The GUI is an integral component of the soft T-UE architecture. Designed to allow users to easily select and configure tests while providing real-time data visualization, the GUI uses Grafana to display key metrics such as UL/DL bitrate, connection status, attack type, and duration. The architecture includes an interprocess communication (IPC) channel that facilitates real-time data exchange between the soft T-UE and the GUI. JSON-encoded messages are used to update the GUI with the current status and operational metrics of the soft T-UE. This interface ensures that users can monitor and analyze tests effectively, enhancing the usability and accessibility of the soft T-UE. Real-time updates and visual feedback are essential for understanding the test outcomes and making informed decisions based on the results.
- **Agents in key O-RAN components:** Strategic deployment of agents within O-RAN deployments enhances the functionality and adaptability of the soft T-UE for rigorous security testing. Leveraging the foundational structure of srsRAN’s UE framework, the soft T-UE augments UE functionalities, message handling, and signaling mechanisms to conduct precise tests on targeted RAN components. These agents are strategically positioned at critical points within the O-RAN architecture, such as xApps, rApps, or the CU/DU, facilitating the execution of custom sequence of machine instructions and seamless data collection in response to UE-side signaling and exchanged packets.

III. TESTING METHODS AND PROCEDURES

The testing methods and procedures supported by the soft T-UE encompass 3GPP Interface testing, O-RAN Alliance test procedures, and custom security test scenarios. These procedures are meticulously designed to evaluate the functionality, conformance, performance, and security of 5G and open RAN components, ensuring a comprehensive and robust testing framework.

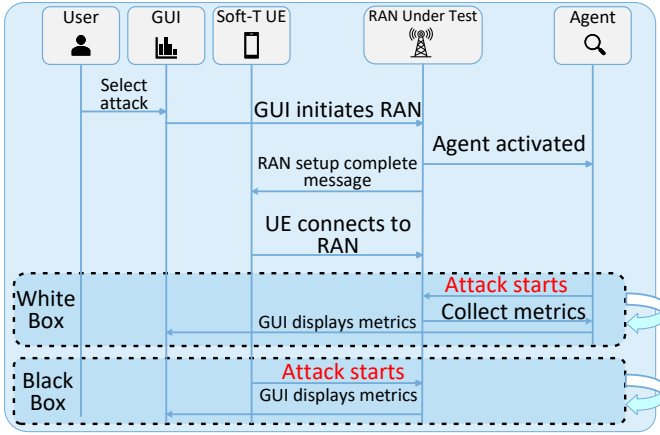


Fig. 2: General Test Flow

A. Test Procedures

- 3GPP Interfaces Testing:** Testing the interfaces specified by 3GPP is crucial for ensuring the security and reliability of 5G networks. These interfaces, such as N1, N2, N3, and others defined by 3GPP, are essential for connecting various network functions and exchanging sensitive data. Extensive vulnerabilities in these interfaces highlight the need for thorough testing [7]. Effective testing procedures aim to verify the integrity, confidentiality, and availability of transmitted data while mitigating potential risks through these interfaces.
- O-RAN Alliance Security Test Specifications:** The soft T-UE incorporates test specifications developed by the O-RAN Alliance’s Working Group 11 (WG11) [8]. These specifications emphasize comprehensive security testing, including vulnerability assessments, penetration testing, and compliance with security requirements. WG11’s frameworks address potential security threats and ensure robust encryption, authentication, and integrity protection mechanisms are in place to safeguard the RAN [9].
- Custom Security Test Scenarios:** The soft T-UE is equipped to support various configurable attack scenarios, including UE fuzzer, DoS, and spoofing attacks. Users can activate specific parameters to test different security aspects of the RAN, allowing the soft T-UE to adapt to emerging threats and evolving security requirements. This flexibility ensures that the soft T-UE can conduct a wide range of tests, from common security evaluations to custom test procedures designed.

B. General Soft T-UE Test Flow

In the following, we detail the flow of a typical test that can be performed via the soft T-UE tool, including how to employ the GUI or CLI to launch a test, test activating process, and obtain logging results for analysis. Depending on whether white box or black box testing is being conducted, the methodology for implying the attack scenario might change. The general flow of deploying the security testing use cases using the soft T-UE is visualized in Fig. 2. The flow can be presented as the following sequence of events:

- Configure Test Parameters:** Users begin by configuring the test parameters via the GUI or CLI. The GUI allows for easy selection and configuration of test scenarios, attack types, and specific parameters to be tested, such as the interval between attack instances and the duration of each attack. The CLI offers similar flexibility, enabling users to set parameters through command-line arguments. After the parameters of interest are configured, the test is launched.
- Establish Connection:** Upon launching the test, the Soft T-UE initiates the connection establishment procedure with the RAN under test. This involves scanning for available networks, selecting the strongest cell, and completing the standard 5G/Open RAN attach and connection procedures.
- Execute Test Scenarios:** Once connected, the soft T-UE executes the configured test scenarios. For white box testing, an agent at the component under test performs the attack. For black box testing, the UE itself performs the attack through signaling and packets exchanged with the RAN.
- Monitor Real-Time Data:** During the test, real-time data is displayed on the GUI or output in the CLI, including UL/DL bitrate, connection status, attack type, duration, and other performance metrics of interest to the specific ongoing test that can be chosen, specifically, at the first step. This real-time feedback allows users to monitor the test progress and performance.
- Data Collection:** Throughout the test, the soft T-UE collects data on various metrics, such as UL/DL bitrate, connection stability, and RAN responses to attacks. This data is logged in JSON format for easy parsing and analysis. For white box testing, an agent in the white box RAN is activated at the component under test to facilitate data collection and communication with the client residing in the RAN. This ensures accurate and comprehensive data capture, enhancing the reliability of the test results. For black box testing, RAN signaling and responses to the soft T-UE packets are collected.
- Data Analysis:** After the test, the collected data is analyzed to evaluate the RAN’s performance and security resilience. The results are documented, and any anomalies or vulnerabilities are identified for further investigation.

IV. SOFT T-UE USE CASE IMPLEMENTATION AND RESULTS

Fuzzing the RRC layer in the UE is a powerful technique to uncover vulnerabilities and ensure robustness in communication protocols. The RRC layer is critical for managing the signaling between the UE and the gNodeB (gNB) in the RAN. This layer handles essential functions such as connection setup, maintenance, reconfiguration, and release. By introducing malformed or unexpected inputs into the RRC messages, fuzzing can identify weaknesses that could be exploited to disrupt network operations, degrade service quality, or compromise security.

When the RRC layer in the UE is subjected to fuzzing, several RAN functions can be significantly impacted. The

gNB, which manages RRC connections with the UE, may encounter malformed RRC connection requests, reconfiguration messages, and connection releases. Such disruptions can cause gNB malfunctions or crashes, compromising the reliability of the network. Fuzzed RRC messages can disrupt the establishment, modification, and release of radio bearers managed by the gNB, causing interruptions in data transmission and signaling. Additionally, handover procedures between cells can be disrupted, resulting in dropped connections and degraded service quality. Security management is another critical area where the gNB's role is vital, and fuzzing RRC messages related to security can potentially compromise the integrity and confidentiality of communications [10].

The impacts of RRC fuzzing extend beyond the RAN to core network components. The Access and Mobility Management Function (AMF), which handles UE registration, deregistration, and mobility management, can experience abnormal behavior due to malformed RRC messages. This can lead to issues with registration, mobility, and session management, causing service disruptions [11]. The AMF is also responsible for authenticating UEs and managing security contexts. Fuzzed RRC messages can interfere with these procedures, potentially leading to security breaches targeting the AMF functionalities and other core network functions, such as the Session Management Function (SMF), Unified Data Management (UDM), and Policy Control Function (PCF).

We specifically targeted the initial UE message registration request for fuzzing to evaluate the robustness of the RRC layer. This focused approach allowed us to assess how the gNB handles unexpected inputs specifically during the registration process, examining its impact on critical functions. During the test, we are utilizing a controlled environment for fuzzing, ensuring that the tests only affect the initial UE message registration request to accurately capture the standalone effect of misconfiguration RRC on the performance of the RAN. This controlled approach ensured systematic testing of the RRC layer under varied conditions, facilitating the identification of vulnerabilities and assessment of network robustness which aligns with recent literature attempting to formalize the fuzzing process [12]. Extensive logging and monitoring were employed to capture and analyze the behavior of both the RAN and core network components during the fuzzing process.

A. Implementation

For the implementation of RRC fuzzing, we utilized SRSRAN Project version 24.4 for the gNB, leveraging an Ettus B210 USRP as the hardware platform. For the UE, we employed the soft-T UE, which was modified from SRS UE version 23.11, also using an Ettus B210 USRP to ensure compatibility and optimal performance. The core network was Open5GS release 17. All software was running on COTS equipment running the latest LTS release of Ubuntu Linux paired with a low-latency kernel. This setup allowed us to simulate and fuzz the RRC messages effectively between the UE and the RAN. The implementation can be seen in Fig. 3 which involved the following procedures executing in order:

- 1) A fuzzer on the soft-T UE specifically targets and manipulates the initial UE message registration request, ensur-

ing comprehensive testing of the RRC layer's handling of registration procedures.

- 2) The fuzzed registration messages are transmitted to the RAN through the Uu interface, allowing for the evaluation of the gNB's response and behavior under various fuzzing conditions.
- 3) Network traffic in the form of PCAP files is captured during the fuzzing process. These PCAP files are then converted to JSON format to facilitate seamless integration and analysis within the GUI.
- 4) Critical metrics such as connection success rates and packet error rates are plotted on the GUI. This provides users with a real-time, visual representation of the system's performance and robustness under various test conditions.

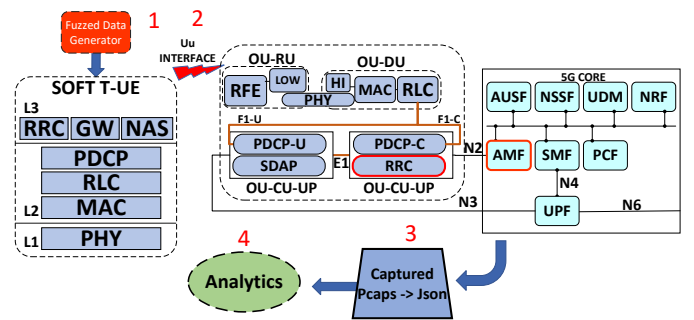


Fig. 3: Fuzzing attack diagram

B. Results Analysis

Fuzzing the RRC layer in the UE reveals how critical the robustness and security of signaling protocols are for the overall stability of the network. We performed fuzzing tests on the initial UE message registration request, focusing on the 26 data bytes (208 bits) that constitute the data portion of the packet. To ensure a thorough analysis, we conducted 100 tests randomly altering a certain number of bits each time. Automating the UE fuzzing process was achieved using a custom controller that initiates the Soft T-UE and the RAN, followed by a modified function for the SDU buffer. This function targets a byte within the SDU buffer data, such as RRC registration request and other RRC messages, and fuzzes one of the 8 bits in that byte to introduce variability and detect potential vulnerabilities. During each test the RAN's response was monitored for anomalies, such as unexpected acceptance of malformed requests, system crashes, or other abnormal behaviors. Our objective was to identify vulnerabilities in the registration process that could be exploited by malicious actors. We measured the impact on registration success rates. Our analysis revealed that only a few bits altered had a disproportionately high impact on successful UE connections which can be seen in Fig. 4. The RRC Setup Complete message, which is 26 bytes in length and contains the RRC Registration Request which is encrypted, underwent bitwise fuzzing as shown in Fig. 5. Each bit within every byte was altered individually, revealing the vulnerability shown from 1

to 100, representing the chance that the UE will still create a PDU session with the corrupted data with 100 being the most likely to still work. This analysis highlights the protocol's significant vulnerability to fuzzing, with a high likelihood of failure for most bits. Furthermore, this result suggests that a targeted fuzzing approach could induce failures more frequently. This comprehensive approach underscores the importance of detailed and systematic testing in uncovering and mitigating potential security weaknesses in essential network operations.

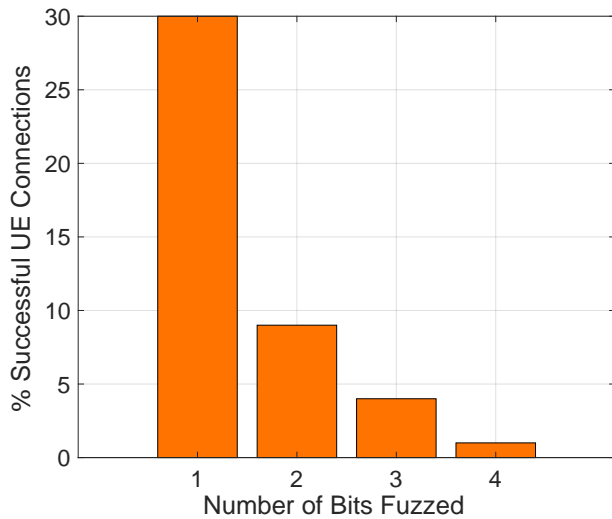


Fig. 4: Effect of fuzzing

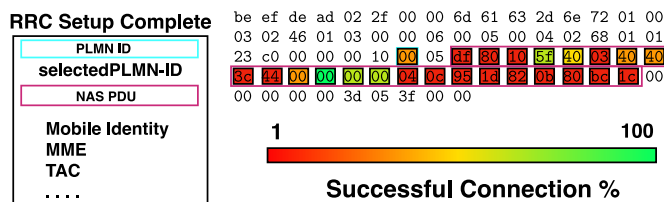


Fig. 5: Vulnerability of bits fuzzed

V. CONCLUSIONS

In conclusion, the rapid advancements in networks necessitate robust and flexible security testing mechanisms. Traditional testing approaches, hindered by high costs and proprietary constraints, are insufficient for the dynamic and complex threat landscape faced by these modern networks. The proposed soft T-UE addresses these challenges by offering a versatile, open-source platform for comprehensive security evaluations. The soft T-UE empowers the assessment of authentication mechanisms, encryption protocols, and the resilience of network components under diverse attack scenarios. The soft T-UE fosters innovation in security measures, enhancing the ability to anticipate and mitigate potential breaches in 5G and O-RAN environments. This paper has outlined the system architecture, detailed the testing methods, and provided implementation specifics, demonstrating the potential of the soft T-UE to significantly improve security testing practices in the rapidly evolving landscape of wireless communications.

ACKNOWLEDGEMENT

This material is based upon work supported by the National Telecommunications and Information Administration (NTIA) under Award No. 28-60-IF012

REFERENCES

- [1] A. S. Abdalla and V. Marojevic, "End-to-end o-ran security architecture, threat surface, coverage, and the case of the open fronthaul," *IEEE Communications Standards Magazine*, vol. 8, no. 1, pp. 36–43, 2024.
- [2] 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 & ai interface," in *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 277–287. [Online]. Available: <https://doi.org/10.1145/3643833.3656118>
- [3] F. Feliana, T.-W. Hung, B. Chen, and R.-G. Cheng, "Evaluation of control/user-plane denial-of-service (dos) attack on o-ran fronthaul interface," 2024.
- [4] S.-H. Liao, C.-W. Lin, F. A. Bimo, and R.-G. Cheng, "Development of c-plane dos attacker for o-ran fhi," in *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, ser. MobiCom '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 850–852. [Online]. Available: <https://doi.org/10.1145/3495243.3558259>
- [5] B. Tang, V. K. Shah, V. Marojevic, and J. H. Reed, "Ai testing framework for next-g o-ran networks: Requirements, design, and research opportunities," *IEEE Wireless Communications*, vol. 30, no. 1, pp. 70–77, 2023.
- [6] X. Foukas, B. Radunovic, M. Balkwill, and Z. Lai, *Taking 5G RAN Analytics and Control to a New Level*. New York, NY, USA: Association for Computing Machinery, 2023. [Online]. Available: <https://doi.org/10.1145/3570361.3592493>
- [7] M. Mahyoub, A. AbdulGhaffar, E. Alalade, E. Ndubisi, and A. Matrawy, "Security analysis of critical 5g interfaces," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2024.
- [8] 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 Network*, vol. 36, no. 6, pp. 206–213, 2022.
- [9] "O-RAN security test specifications 7.0," O-RAN Alliance, Tech. Rep., Jun. 2024. [Online]. Available: <https://o-ran.org/documents>
- [10] K. Baccar and A. Lahmadi, "An experimental testbed for 5g network security assessment," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, 2023, pp. 1–6.
- [11] F. Mancini, S. Da Canal, and G. Bianchi, "Amfuzz: Black-box fuzzing of 5g core networks," in *2024 19th Wireless On-Demand Network Systems and Services Conference (WONS)*, 2024, pp. 17–24.
- [12] 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. 29 175–29 193, 2024.

BIOGRAPHIES

Joshua Moore (jjm702@msstate.edu) is a PhD student in the Department of Electrical and Computer Engineering at Mississippi State University, Starkville, MS, USA. His research interests include O-RAN, 5G/next-G communications, and RAN Management and Orchestration.

Aly Sabri Abdalla (asa298@msstate.edu) is an Assistant Research Professor in the Department of Electrical and Computer Engineering at Mississippi State University, Starkville, MS, USA. His research interests are on wireless communication and networking, software radio, spectrum sharing, wireless testbeds and testing, and wireless security with application to mission-critical communications, open radio access network (O-RAN), unmanned aerial vehicles (UAVs), and reconfigurable intelligent surfaces (RISs).

Charles Ueltschey (cmu32@msstate.edu) is an undergraduate student in computer science at Mississippi State University, Starkville MS, USA. His research interests are Wireless communications, O-RAN security, and Machine Learning.

Vuk Marojevic (vuk.marojevic@msstate.edu) is an associate professor in electrical and computer engineering at Mississippi State University, Starkville, MS, USA. His research interests include resource management, vehicle-to-everything communications and wireless security with application to cellular communications, mission-critical networks, and unmanned aircraft systems.