

Monitoring 5G Core Networks Vulnerabilities with eBPF

Gabriele Nunziati^{1b}, Claudio Fiandrino^{2b}, *Member, IEEE*, Luca Foschini^{1b}, *Senior Member, IEEE*, and Paolo Bellavista^{1b}, *Senior Member, IEEE*

Abstract—The current design of 5G Core Network (5G CN) adopts a cloud-native service-based architecture, where Network Functions (NFs) are exposed as services that can be dynamically composed and managed to achieve high flexibility. These NFs are interconnected via interfaces that Standardization Development Organizations (SDOs) like 3GPP have standardized. The complexity of the interconnections and data sensitivity make these interfaces vulnerable. In this letter, we advocate the use of extended Berkeley Packet Filter (eBPF) to monitor the 5G CN interfaces activities. eBPF programs run in kernel space of the host machine, thereby providing visibility of all programs and this is especially convenient for observability of 5G CN NFs. With a specific use case implemented in Open Air Interface (OAI), we demonstrate the benefits of the eBPF framework to identify session deletion attacks and mitigate associated risks.

Index Terms—5G core network, interface vulnerability, eBPF

I. INTRODUCTION

THE core network is a key component of mobile networks as enables data communication between end-user devices accessing the mobile network via the Radio Access Network (RAN) and public networks like the Internet. Its main functions encompass user-level functions such as traffic steering, session and Quality of Service (QoS) management, as well as control plane functions such as signaling, mobility management, initial access, and authentication. The core network of 5G systems relies on virtualized network functions, usually deployed in the cloud over commodity hardware [1], [2], integrated via a Service Based Architecture (SBA) using Service Based Interfaces (SBIs) to provide interconnection between Network Functions (NFs). The approach enables high flexibility and enables logically independent services, i.e., slices, vis-a-vis the previous generations of core networks [3], [4], [5].

The transition from a non-virtualized to a virtualized core network posed significant challenges in its inception in pre-5G technology. For example, signaling storms during peak usage periods led to delays in event processing, service disruptions, and degraded user experience [6]. The challenges in 5G systems grow more complex with the increasing complexity of network functions that are becoming more and more specific, the growing volume of traffic, and the potential for failures in

hardware, software, or network infrastructure [7]. The SBA and SBI, while allowing for high flexibility, also introduce a variety of vulnerabilities that can be exploited to disrupt services, steal sensitive data, and compromise user privacy [8]. A recent work remarks that even one vulnerability in the core can persistently disrupt all cellular communications (phone calls, messaging and data) at a city-wide level [9].

With the overarching goal of identifying vulnerabilities in the 5G protocol stack, the researchers have utilized diverse techniques in the recent years. For instance, 5GReasoner uses formal verification to analyze control-plane protocols [10]. 5GCVerif uses model-based testing to evaluate vulnerabilities that can lead to unauthorized access and denial-of-service attacks in the access control of the 5G Core Network (5G CN) [11]. In [12], the authors use static program analysis to compare NFs 5G core implementations and the 3GPP specifications, uncovering previously unknown instances of over-privilege that can compromise security and privacy. Finally, neural networks like LSTM can predict traffic patterns and detect anomalous signaling [13].

In this letter, we explore a different and novel approach. Specifically, we propose to use extended Berkeley Packet Filter (eBPF) to monitor the 5G CN interfaces activities, to identify potential attacks, and to develop effective countermeasures. We took inspiration from Janus [14] that leverages eBPF to allow third-party developers to load custom code directly into RAN functions, enabling fine-grained, flexible and efficient monitoring and control. Some other seminal efforts use eBPF in cloud-native environments, including the case of 5G and 6G mobile networks [15], [16].

In particular, we demonstrate the benefit of using eBPF for practical monitoring purposes for a relevant use case. Specifically, we originally target a key interface in the 5G CN, i.e., the N4 interface. Through this interface, the Session Management Function (SMF) manages user sessions and enforces QoS policies, based on user requirements and network conditions. Protecting the Packet Forwarding Control Protocol (PFCP) used in the N4 interface is key to prevent attackers from manipulating user sessions, intercept sensitive data, or degrade network performance. For the sake of demonstration, we implement on Open Air Interface (OAI) a Denial of Service (DoS) attack via the PFCP Session Deletion Requests that would disrupt the Protocol Data Unit (PDU) session between the User Equipments (UEs) that are the target of the attack and the data network without having them to be disconnected from the RAN. Our eBPF monitoring routine identifies these malicious requests and is capable of restoring the UEs' connectivity. While we focus for demonstration

This work is partially supported by bRAIN (PID2021-128250NB-I00) and 6G-ELSA (PID2022-136769NB-I00) projects funded by MCIN/ AEI /10.13039/501100011033/ and the European Union ERDF "A way of making Europe"; C. Fiandrino is a Ramón y Cajal awardee (RYC2022-036375-I), funded by MCIU/AEI/10.13039/501100011033 and the ESF+.

G. Nunziati, L. Foschini and Paolo Bellavista are with the University of Bologna, Bologna, Italy. E-mail: {firstname.lastname}@unibo.it

C. Fiandrino is with IMDEA Networks Institute, Madrid, Spain. E-mail: {claudio.fiandrino}@imdea.org.

Manuscript received April 30, 2025; revised June 4, 2025.

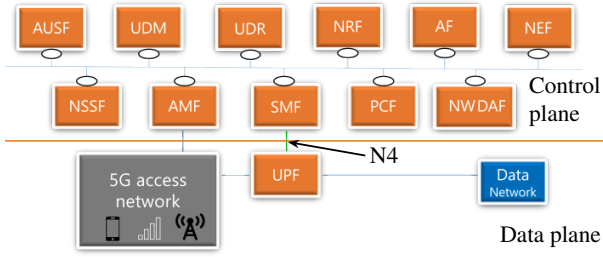


Fig. 1. The 5G CN architecture with a focus on the N4 interface

purposes on malicious Session Deletion Requests, note that monitoring with eBPF is general and applicable to any other vulnerability of 5G CN interfaces [8].

II. A PRIMER ON THE 5G CORE ARCHITECTURE

In this section, we report background material and detail the focus of this letter. We use Figure 1 to guide the presentation of the relevant NFs and interfaces hereafter summarized.

Network Functions. The 5G CN is split into Control Plane (CP) and User Plane (UP). The CP exchanges signaling traffic across NFs while the UP takes care of data traffic. The Access and Mobility Function (AMF) serves as the initial point of contact for UEs, taking them through the registration and authentication process with the network. The SMF manages user sessions, assigns IP addresses, and coordinates with the User Plane Function (UPF) to ensure proper network connectivity. The UPF acts as the gateway between the UE and external networks, being the only UP NF handling data traffic. Other network functions, such as the Unified Data Management (UDM), Policy Control Function (PCF), Network Exposure Function (NEF), Application Function (AF), Network Slicing Selection Function (NSSF), and Location Management Function (LMF) [7] provide various services and manage user interactions within the 5G CN.

Interfaces. Each of these NF, also known as end points, is interconnected with other NFs via interfaces. Interfaces starting with “N” connect different network elements: N1 (UE-AMF), N2 (5G-AN-AMF), N3 (5G-AN-UPF), N4 (SMF-UPF), N6 (UPF-data network), and N9 (UPF-UPF) among the others. N1 combines the radio interface (Uu) with N2 for functionalities like registration and message services. Xn connects next Generation Node Bs (gNBs) for handover, data forwarding, and control. F1 connects gNB functional splits (Distributed Unit (DU) and Central Unit (CU)) for control and user traffic signaling. Service Based Interfaces (SBI) represent an API-based interface for communication between network functions within the 5G core.

Our Focus in This Letter. The survey in [8] thoroughly reviews vulnerabilities across these interfaces. This letter demonstrates that monitoring NFs and interfaces with eBPF enhances the 5G CN’s operational robustness. We focus on the N4 interface, which connects the SMF and UPF, exchanging sensitive signaling data such as QoS parameters and traffic handling rules—making it critical for session management. The PFCP protocol operates at the N4 interface, managing control and forwarding between CP and UP. It establishes, modifies,

and deletes sessions to ensure efficient packet processing and routing based on SMF instructions.

III. MONITORING 5G INTERFACE ACTIVITIES WITH eBPF

The Choice of eBPF. eBPF is a technology that enables application developers to enhance the capabilities of the operating system kernel without modifying its source code. It makes it possible for sandboxed programs to execute within the kernel environment and enables observability, security, and networking functions. eBPF programs are event-driven and can be written in a high-level language, making them easy to develop and deploy.

In this letter, we show how to ensure resilience in the 5G CN interface activities with two modules: eBPF Detection Program (EDP) is responsible for attack detection, and Protocol Compliance Protector (PCP) handles attack mitigation. Next, we introduce the DoS attack, the EDP, and, finally, the PCP modules. Figure 2 illustrates the entire procedure and we will use it hereafter to guide the reader through the procedure.

The Attack. A legitimate Session Deletion Request starts when a UE wants to disconnect from the network. The request for PDU termination goes through the AMF, which triggers the SMF to send the Session Deletion Request to the UPF. The UPF identifies the session to be deleted by matching the Session Identifier (SEID) with the one contained in the Session Deletion Request.

In the attack, the compromised SMF upon triggered to send a legitimate Session Deletion Request for a target UE, sends multiple of them including the SEID information of other UEs. The UPF upon receiving all these requests, simply terminates those sessions while the AMF remains unaware, i.e., the GTP-U tunnel is still active although the UEs do not have connectivity with the data network.

eBPF Observability with EDP. EDP executes the eBPF-based detection routine that examines the control traffic on the 5G CN and detects anomalies. The eBPF program first filters all PFCP packets with Session Deletion Request and based on a timer distinguishes between legitimate and non-legitimate requests. The DoS attack sends a batch of requests back-to-back and in real mobile networks is unusual that so many UEs de-register with such short notice [17]. EDP is implemented as a C-defined eBPF routine using BPF Compiler Collection toolkit and the type of eBPF program is a socket filter. The key advantage of EDP lies in its minimal overhead: unlike traditional deep packet inspection methods, which are resource-intensive, the use of eBPF enables a selective event tracing and aggregation that minimizes the data collection overhead.

Attack Mitigation with PCP. When EDP reads a Session Deletion Request from raw socket and deems it as malicious, the PCP module kicks-in and looks-up the affected UE via its SEID. Using the SEID, the PCP module then triggers PFCP Session Establishment Request to re-establish the disrupted sessions of the affected UEs. The PCP module is implemented as a Python script that interacts with EDP and enables an automated reaction to the attack.

Limitations. Due to the exploratory nature of this work, we use socket filters due to their simplicity and efficiency in

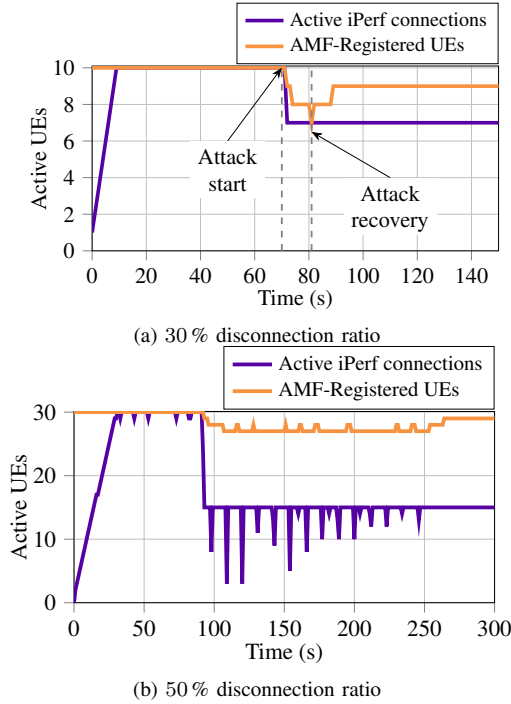


Fig. 4. Effects of a malicious Session Deletion Request and recover made possible by the eBPF monitoring framework

Request whose objective is to disconnect a fraction of the UEs in addition to a legitimate one. Fig. 4 shows that the DoS attack is successful as when it is executed both iPerf connections and the number of UEs registered in the AMF drop. Our eBPF framework is capable to detect such a malicious Session Deletion Request as detailed in §III and triggers a recovery action. In the recovery phase, all the UEs that were illegitimately disconnected are registered again in the 5G CN and this becomes evident because the number of UEs registered with the AMF increases. Obviously, the user that was supposed to be legitimately disconnected is not registered again. Please note that obviously, without intervention that is external to the capabilities of the 5G CN, it is not possible to restore the application (i.e., the iPerf connections). Finally, Fig. 4(b) shows that the profile of the iPerf connections is irregular. This is an artifact completely unrelated to the attack. It is due to the limited computing resources and makes these connections to experience brief interruptions.

V. CONCLUDING REMARKS

In this letter, we showed the benefits of using eBPF as an enabler for monitoring activities on the 5G CN interfaces. Specifically, we considered the case of the N4 interface that interconnects the SMF and the UPF and showed that eBPF makes it possible to spot illegitimate UEs disconnection due to malicious Session Deletion Requests. We implemented and validated the monitoring framework on OAI, a reference 5G open-source software platform designed for experimentation, prototyping, and research in the field.

Future work will focus on extending our eBPF-based monitoring framework to incorporate XDP and tracing programs. This will enable us to capture richer contextual information to detect more complex attack patterns and evaluate additional

metrics other than UE disconnection rate like latency and recovery speed. We will also investigate the integration of AI/ML techniques to analyze the collected data and further enhance the detection of anomalous activities.

REFERENCES

- [1] J. Larrea, A. E. Ferguson, and M. K. Marina, “CoreKube: An efficient, autoscaling and resilient mobile core system,” in *ACM MobiCom*, 2023.
- [2] A. Kumar, P. Naik, S. Patki, P. Chaudhary, and M. Vutukuru, “Evaluating network stacks for the virtualized mobile packet core,” in *Proc. of ACM APNet*, 2022, p. 72–79.
- [3] S. Vittal, S. Sarkar, and A. A. Franklin, “Revamping the resilience and high availability of 5G core for 6G ready network slices,” *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 2287–2302, 2024.
- [4] P. Sharma, T. Atalay, H. Andrew Gibbs, D. Stojadinovic, A. Stavrou, and H. Wang, “5G-WAVE: A core network framework with decentralized authorization for network slices,” in *Proc. of IEEE INFOCOM*, 2024, p. 1–10.
- [5] C. H. T. Arteaga, A. Ordoñez, and O. M. C. Rendon, “Scalability and performance analysis in 5G core network slicing,” *IEEE Access*, vol. 8, pp. 142 086–142 100, 2020.
- [6] M. T. Raza, D. Kim, K.-H. Kim, S. Lu, and M. Gerla, “Rethinking LTE network functions virtualization,” in *Proc. IEEE ICNP*, 2017, pp. 1–10.
- [7] A. Pinto, G. Santaromita, C. Fiandrino, D. Giustiniano, and F. Esposito, “Characterizing location management function performance in 5G core networks,” in *Proc. of IEEE NFV-SDN*, 2022, pp. 66–71.
- [8] 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.
- [9] N. Bennett, W. Zhu, B. Simon, R. Kennedy, W. Enck, P. Traynor, and K. R. B. Butler, “RANSacked: A domain-informed approach for fuzzing LTE and 5G RAN-core interfaces,” in *Proc. of ACM CCS*, New York, NY, USA, 2024, p. 2027–2041.
- [10] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, “5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol,” in *Proc. of ACM CCS*, 2019, p. 669–684.
- [11] M. Akon, T. Yang, Y. Dong, and S. R. Hussain, “Formal analysis of access control mechanism of 5G core network,” in *Proc. of ACM CCS*, 2023, p. 666–680.
- [12] S. Thorn, K. V. English, K. R. B. Butler, and W. Enck, “5GAC-Analyzer: Identifying over-privilege between 5G core network functions,” in *Proc. of ACM WiSec*, 2024, p. 66–77.
- [13] R. Pell, M. Shojafar, and S. Moschioniannis, “LSTM based anomaly detection of PFPC signaling attacks in 5G networks,” *IEEE Consumer Electronics Magazine*, pp. 1–9, 2024.
- [14] *Taking 5G RAN Analytics and Control to a New Level*, 2023.
- [15] S. Miano, F. Risso, M. V. Bernal, M. Bertrone, and Y. Lu, “A framework for eBPF-based network functions in an era of microservices,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 133–151, 2021.
- [16] D. Soldani, P. Nahi, H. Bour, S. Jafarizadeh, M. F. Soliman, L. Di Giovanna, F. Monaco, G. Ognibene, and F. Risso, “eBPF: A new approach to cloud-native observability, networking and security for current (5G) and future mobile networks (6G and beyond),” *IEEE Access*, vol. 11, pp. 57 174–57 202, 2023.
- [17] G. Attanasio, C. Fiandrino, M. Fiore, J. Widmer, N. Ludant, B. Bloessl, K. Kousias, Özgü Alay, L. Jacquot, and R. Stanica, “In-depth study of RNTI management in mobile networks: Allocation strategies and implications on data trace analysis,” *Computer Networks*, vol. 219, p. 109428, 2022.
- [18] T. Høiland-Jørgensen, J. D. Brouer, D. Borkmann, J. Fastabend, T. Herbert, D. Ahern, and D. Miller, “The express data path: fast programmable packet processing in the operating system kernel,” in *Proc. of ACM CoNEXT*, 2018, p. 54–66.
- [19] F. Kaltenberger, A. P. Silva, A. Gosain, L. Wang, and T.-T. Nguyen, “OpenAirInterface: Democratizing innovation in the 5G era,” *Computer Networks*, vol. 176, p. 107284, 2020.
- [20] P. F. Fernández Pérez, C. Fiandrino, and J. Widmer, “Characterizing and modeling mobile networks user traffic at millisecond level,” in *Proc. of ACM WINTech*, 2023, p. 64–71.