POSTER: Accountable Cross-Operator 5G Charging via TEEs

Mijin Shin
Sungshin Women's University
Seoul, South Korea

Wooram Park
Kyung Hee University
Yongin, South Korea

Sangwook Bae
Cape
Washington, DC, USA

CheolJun Park*
Kyung Hee University
Yongin, South Korea

Seongmin Kim*
Sungshin Women's University
Seoul, South Korea

Abstract

The 5G core network's control plane operates under a trust-based model. While this model is sufficient for single-operator deployments, it breaks down in cross-operator settings, such as Local Breakout (LBO) roaming and light MVNO-based network sharing. In this work, we revisit this trust assumption from a charging accountability perspective. We systematically identify key attack surfaces in cross-operator charging workflows by analyzing charging-relevant operations across network functions, where cross-operator visibility is inherently limited. Based on these insights, we derive design goals for accountable charging and outline a Trusted Execution Environment (TEE)-based approach that enables verifiable execution of charging-critical functions. We further develop a roaming testbed using Open5GS integrated with an online charging system, and conduct a preliminary evaluation of the TEE-based approach by measuring its overhead on charging-critical operations.

ACM Reference Format:
Mijin Shin, Wooram Park, Sangwook Bae, CheolJun Park, and Seongmin Kim. 2026. POSTER: Accountable Cross-Operator 5G Charging via TEEs. In *Proceedings of the 19th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '26), June 30-July 03, 2026, Saarbrücken, Germany.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3765613.3814570

1 Introduction

Mobile cellular services operate across multiple operators, where roaming enables a home operator to rely on a visited network to deliver services, effectively outsourcing traffic handling and control-plane operations. In 3GPP roaming, while Home Routing (HR) retains control within the home network, LBO delegates both traffic handling and control-plane execution to the visited network, improving performance but leaving the home operator without visibility into how these operations are executed [1–3].

As a result, critical internal messages (e.g., policy enforcement, traffic handling, and usage reporting) are implicitly trusted without independent verification or accountability. The issue is particularly severe in LBO and light MVNO or infrastructure-sharing scenarios, where control is fully externalized.

*Co-corresponding authors

WiSec '26, Saarbrücken, Germany

ACM ISBN 979-8-4007-2201-1/2026/06
https://doi.org/10.1145/3765613.3814570

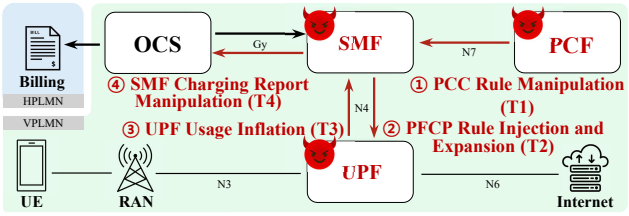

Fig. 1: Charging workflow and attack surfaces in LBO-based cross-operator 5G roaming.

Among these, charging is critical, as it directly impacts monetary settlement [5]. In LBO, usage is measured and reported by the visited network and accepted for billing without independent verification, creating opportunities for charging manipulation, such as incorrect usage accounting or tampering with charging reports. This raises a fundamental question: *How can an operator trust and pay for network usage when it cannot verify how the charges were computed?*

In this work, we study a TEE-based approach to enable accountable charging in cross-operator 5G roaming by protecting charging-critical control-plane execution against fraud arising from the lack of verifiable visibility. To this end, we first identify charging-related threats by analyzing how charging-critical operations are distributed across network functions in cross-operator roaming, and enumerate key attack surfaces arising from inconsistencies in policy enforcement, traffic measurement, and usage reporting. We then develop an Open5GS-based roaming testbed integrated with an online charging system [6, 7], which enables systematic analysis of these attack surfaces and their impact on charging outcomes. Finally, we derive design goals for accountable charging and outline a TEE-based architecture for verifiable execution of charging-critical control-plane functions across operator boundaries.

2 Threat Model and Attack Scenarios

While similar challenges may arise in other cross-operator deployments such as light MVNO settings, we focus on LBO as a representative scenario where control-plane delegation is most explicit.

Threat model. We consider a cross-operator 5G deployment under LBO-based roaming, where charging-related functions—such as policy enforcement, traffic measurement, and usage reporting—are executed within the *visited network*. In this setting, the *home operator* has no direct visibility into data-plane traffic or the execution of charging logic, and must rely on charging outcomes reported by the *visited network*.

Charging workflow overview. As illustrated in Fig. 1, charging in LBO follows a multi-stage workflow across network functions. The policy control function (PCF) generates policy and charging control

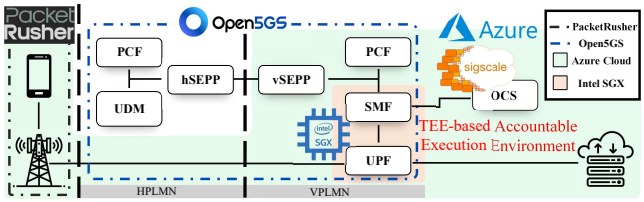

Fig. 2: Prototype LBO roaming testbed.

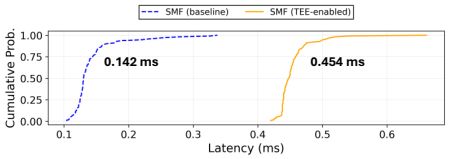

Fig. 3: Comparable baseline and SGX for UE.

(PCC) rules, which are translated by the session management function (SMF) into forwarding and usage reporting rules (PFCP) for the user plane function (UPF). The UPF measures traffic and produces usage reports, which are aggregated by the SMF and forwarded to the charging backend (e.g., OCS/CHF). This distributed workflow creates multiple points where charging outcomes can be influenced without direct visibility from the home operator.

Attack scenarios. Under this model, we identify key attack surfaces across the charging workflow, each corresponding to a different stage of control-plane execution.

T1: PCC Rule Manipulation. A visited PCF can modify charging-relevant PCC rules, creating discrepancies between intended and enforced policies. In particular, QoS or monitoring parameters can be altered to enable unauthorized usage or bypass limits.

T2: PFCP Rule Injection and Expansion. A visited SMF can manipulate PFCP rules by injecting additional usage reporting rules or broadening traffic matching conditions. This leads to duplicated charging triggers or unintended traffic classification, resulting in overcharging or misattribution of usage.

T3: UPF Usage Inflation. A visited UPF can manipulate traffic metering by inflating counters or distorting measurement thresholds. As these measurements are directly used for charging, such manipulation results in incorrect usage reports without requiring protocol violations.

T4: SMF Charging Report Manipulation. A visited SMF can alter, duplicate, or suppress usage reports before forwarding them to the charging backend (e.g., OCS/CHF). This directly impacts billing outcomes while remaining opaque to the home operator.

Note that these attack scenarios directly align with threat categories defined in the MITRE FiGHT framework [5]. Building on this alignment, our workflow-driven analysis further refines these categories into concrete, charging-specific attack surfaces under limited cross-operator visibility.

3 TEE-Based Accountable Charging

The core challenge in cross-operator charging is the lack of verifiable visibility into how charging-critical functions are executed in the visited network. We address this by proposing a TEE-based accountable charging architecture in which TEEs provide hardware-isolated execution for charging-critical logic and enable the home operator to verify the operational integrity of the NFs with respect to agreed charging-integrity predicates.

Key idea: attested charging execution. Charging-critical NFs in the visited network are remotely attested to prove that they are running approved code and configuration, and their charging-relevant actions emit compact attested evidence for predicate verification. The home operator checks these records against charging-integrity predicates corresponding to T1–T4. For example, the PFCP derivation predicate requires that each PFCP rule set be derived from an attested PCC input and satisfy auditable constraints (e.g., a bounded number of URRs per charging context), enabling detection of rule injection or over-broad matching.

Discussion. Real-world deployment introduces several design challenges due to TEE and cellular limitations. In particular, commodity-TEE remote attestation mainly verifies launch-time integrity, while accountable charging requires predicate-based runtime evidence for charging-critical transitions. Moreover, placing large NF codebases inside TEEs can incur unnecessary overhead, motivating isolation of only the charging-critical path. We leave this for future work.

4 Preliminary Evaluation

Testbed setup. We implement an LBO roaming testbed using Open5GS [6], as shown in Fig. 2, deploying charging functions in the visited network and the charging backend in the home network. Since Open5GS lacks native 5G charging support, we integrate an external OCS, *SigScale* [7], via the Gy interface. We use PacketRusher [4] to generate UE traffic. The VPLMN runs on SGX-capable Microsoft Azure instances (Intel Xeon(R) Platinum 8370C CPU, 16GB memory), while the HPLMN runs on a separate host (Intel Core i9-10900K), both using Linux kernel 5.15.0-139.

Overhead measurement. To quantify the overhead introduced by TEEs, we measure the handler-level processing latency of PFCP session report request messages in the Open5GS SMF. As shown in Fig. 3, the average processing latency in the non-SGX environment is 0.142 ms, whereas the SGX-based execution exhibits an increased average latency of 0.454 ms (3.2x). This overhead reflects a naive TEE port and a handler-level measurement on the SMF, rather than end-to-end control-plane latency. In practice, its impact is expected to be amortized by network delay between NFs.

Acknowledgement

This work was supported by Institute of IITP grant funded by the Korea government (MSIT) (IITP-2026-RS-2023-00266615 and No.IITP-2026-RS-2024-00437252), and was partially supported by the NRF grant funded by the Korea government (MSIT) (No. RS-2024-00351898 and No. RS-2025-02263915).

References

[1] 3GPP. 2026. Procedures for the 5G System (5GS). TS 23.502. Rel. 17.
[2] 3GPP. 2026. System Architecture for the 5G System (5GS). TS 23.501. Rel. 17.
[3] GSMA. 2026. IMS Roaming and Interworking Guidelines. IR.65.
[4] Hewlett Packard. 2024. PacketRusher. https://github.com/HewlettPackard/PacketRusher. Accessed: 2026-04-10.
[5] MITRE. 2026. MITRE FiGHT: 5G Threat Framework. https://fight.mitre.org/.
[6] Open5GS. 2024. Open Source Implementation for 5G Core and EPC. https://open5gs.org/.
[7] SigScale. 2026. SigScale OCS: Open Source Online Charging System. https://github.com/sigscale/ocs.