On using Blockchain in beyond 5G: Roaming Improvements

Stavros Dimou, Kostas Choumas and Thanasis Korakis
Dept. of ECE, University of Thessaly, Volos, Greece
Email: dstavros, kohoumas, korakis@uth.gr

***Abstract*—The deployment of fifth generation (5G) cellular network technology all around the globe has sparked a new wave of interest in the ability of blockchain to automate and optimize different networking use cases. Such examples are the existing roaming models, which require communication between the Mobile Network Operators (MNOs) when a device has to be authorized by a different MNO than its own. This communication may lead to data privacy concerns and poor service quality due to delays in data transfer. This paper presents a blockchain-based roaming subscriber authentication and registration system for MNOs that uses smart contracts to deliver efficient roaming services. This system establishes dynamic and automatic agreements between MNOs, greatly lowering communication latency and maintaining security and privacy during message exchange.**

***Index Terms*—Blockchain, 5G Networks, Roaming.**

I. Introduction

By 2027, 5G roaming connections are expected to reach 526 million, a sharp increase from 53 million in 2023 [1]. However, Mobile Network Operators (MNOs) face challenges in managing roaming services efficiently, despite rising customer numbers and revenue. One key issue is the inefficient data sharing and reduced performance when a roaming subscriber connects. This occurs because the Visited Public Land Mobile Network (V-PLMN) must communicate directly with Network Functions (NFs) of the Home Public Land Mobile Network (H-PLMN)[1] to access sensitive User Equipment (UE) data and report events.

Blockchain-based applications are now more accessible due to the rapid development of blockchain technologies. As a Distributed Ledger Technology (DLT), blockchain offers decentralization through its consensus mechanism and smart contracts, increasing trust and transparency. In 5G networks, blockchain can reduce data exchange delays and enhance transparency as in [2], with potential for further improvement as noted in [3]. However, its establishment faces challenges from the reluctance of MNOs to share personal information.

This paper introduces a blockchain-based framework for MNOs to securely conduct peer-to-peer transactions with smart contracts, simplifying roaming and improving the authentication and registration of roaming subscribers. The rest of the paper is organized as follows: Section II gives a concise overview of the current roaming models and the difficulties they encounter, while Section III focuses on the suggested blockchain-based improvements on these models.

II. Roaming in 5G Networks

An essential component of 3GPP is roaming, which enables mobile users to use services of an MNO on other PLMNs both domestically (national roaming) and internationally (international roaming). Subscribers must move from their home network (H-PLMN) to a visited network (V-PLMN) under agreements for billing, authentication, and more. Both national and international roaming follow the 3GPP standards with a consistent model, regardless of the H-PLMN and V-PLMN interfaces. This model involves roaming subscribers (UEs) connecting to the 5G Access Network, which provides services through the 5G Core Network (5G-CN). The 5G-CN employs a cloud-based Service-Based Architecture (SBA), necessitating complex interconnections of various NFs.

Roaming-related NFs encompass the Access & Mobility Management Function (AMF) in 5G-CN, responsible for connection and mobility tasks. The AMF authenticates UEs through the Authentication Server Function (AUSF), with authentication credentials provided by the Unified Data Management (UDM). The Packet Data Unit (PDU) session-related operations are handled by the Session Management Function (SMF), and the Policy Control Function (PCF) provides policy rules for control plane functions, including network roaming. During data transfer, the User Plane Function (UPF) is pivotal, bridging the data network and mobile infrastructure. The Network Repository Function (NRF) facilitates discovery for NFs to access up-to-date service information. Finally, the point-to-point interconnections of the NFs (even belonging to different PLMNs) are referred with NX, where X stands for a physical number (e.g. $N24$ refers to the interconnection between H-PCF and V-PCF).

Currently, 5G supports two different roaming models [4].

1) **Home-Routed (HR):** Roaming UEs receive IP addresses from their H-PLMN, with traffic consistently routed via the same PLMN. The main drawback of this model is the high latency it incurs, especially for user plane traffic towards the H-PLMN. However, it is recommended for scenarios with limited trust between MNOs.
2) **Local-Breakout (LBO):** It mitigates HR approach latency issues by having roaming UEs served directly by a V-PLMN. H-PLMNs handle authentication and subscription data exclusively. V-PCF enforces roaming policies and charges per agreement. MNOs relinquish customer control but gain more efficient, latency-focused routing.

Both models can be greatly enhanced by blockchain, especially in the case of UE Authentication-Registration, which is a characteristic shared by both models. Over the 5G-CN, UEs may be authorized in two distinct ways. Either by sending a Subscription Concealed Identifier (**SUCI**) or by sending a 5G introduced Globally Unique Temporary Identity (**GUTI**), which has been allocated to the UE by AMF. SUCI, an encrypted Subscription Permanent Identifier (SUPI), serves for initial UE authentication, while GUTI is a temporary identifier for a limited number of re-authentications, designed to enhance

[1] From now on, ‘H-’ refers to Home and ‘V-’ to Visited.

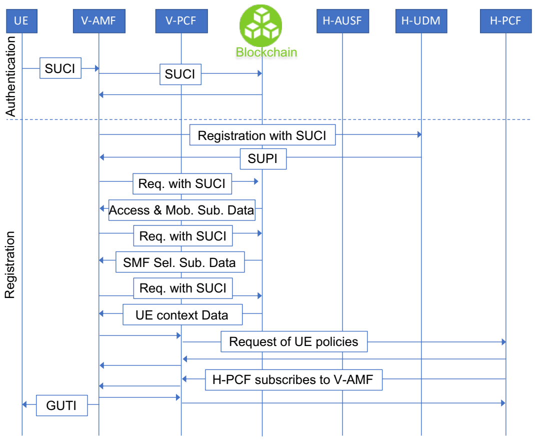

Fig. 1. Blockchain-based Authentication-Registration procedure.

network privacy.

1) Permanent Identity Authentication (using SUCI): When a UE tries to authenticate for the first time, it initially communicates with the V-AMF [5], transmitting its SUCI. The V-AMF is then responsible for communicating with H-AUSF, through the N12 reference point, which is found through the synergy of V-NRF and H-NRF. After H-AUSF obtains the authentication data from H-UDM, through the local N13 reference point, it returns the SUPI to V-AMF, so that it can complete the UE authentication. In total, the **UE authentication requires a single bi-directional message exchange** between V-PLMN and H-PLMN.

2) Temporary Identity Authentication (using GUTI): After the initial authentication of UE with a V-PLMN, V-AMF generates a GUTI that is mapped with the SUPI and keeps this mapping for further re-authentications or PDU session requests.

3) Registration (using SUPI): After authentication, V-AMF exchanges messages with H-UDM, through the N8 reference point, four times during the registration process. The **UE registration requires four extra bi-directional message exchanges** between V-PLMN and H-PLMN. In the course of the first exchange of messages, V-AMF registers with H-UDM, while on the following interchanges, H-UDM provides V-AMF with different data regarding the UE. Finally, the GUTI and a confirmation of the acceptance of the registration request are sent by V-AMF to the UE along with the Registration Request acceptance.

III. Blockchain-based Roaming Models

Reevaluating data sharing among MNOs is crucial in assessing current roaming schemes. Enhancing the performance of such models involves the efficient transfer of agreements, subscriber activity records, and TXs among MNOs. Our proposed framework leverages permissioned blockchains, enabling trustworthy information exchange among MNOs, using a consortium blockchain. Peer attributes are acquired by NFs in order to query and update the ledger, while smart contracts are employed to handle user roaming records. In this Section, a redesigned and improved Authentication-Registration procedure is presented, utilizing blockchain to its fullest potential, as depicted in Figure 1.

1) Permanent Identity Authentication (using SUCI Smart Contract): In an ideal scenario, a smart contract should offer SUPIs of new UEs for direct access by V-PLMN, as in [6]. However, due to privacy concerns, MNOs often cannot share such data, so the proposed model introduces the SUCI smart contract. When executed by H-UDM, it sends write TXs containing numerous SUCIs of the UEs, instead of SUPIs, to the distributed ledger. After a UE tries to connect to V-PLMN, the corresponding V-AMF would query the respective data from its copy of the distributed ledger, **avoiding the bi-directional message exchange** between V-PLMN and H-PLMN. The authentication is complete if the equivalent SUCI value is found.

2) Temporary Identity Authentication (using GUTI Smart Contract): As per [7], GUTI-to-SUPI mapping from V-AMF can be stored in the blockchain for future authentication. Instead, the suggested model adopts a GUTI-to-SUCI mapping approach, akin to the earlier SUCI smart contract. When a UE sends a GUTI to the V-AMF, the V-AMF checks the blockchain for the corresponding SUCI, with GUTI serving as an identifier.

3) Registration Smart Contracts: The four message exchanges between V-AMF and H-UDM evidently increase network latency, and since V-PLMN does not know the SUPI of the registered UE, the first exchange remains almost the same with minor alterations. Initially, once V-AMF registered with H-UDM, an empty response was returned; now, this message includes the SUPI, giving V-PLMN access for future steps. The **three remaining bi-directional message exchanges** between PLMNs are replaced by three new smart contracts, each responsible for the equivalent data from H-UDM, as depicted in Figure 1. For V-PLMN to query UE data accurately, each smart contract includes an additional identifier field, using SUCI instead of SUPI.

References

[1] https://www.juniperresearch.com/press/juniper-research-forecasts-5g-roaming-connections/.

[2] Christopher Harris. Improving Telecom Industry Processes Using Ordered Transactions in Hyperledger Fabric. In *Proc. of IEEE Globecom Workshops*, 2019.

[3] Stavros Dimou, Kostas Choumas, and Thanasis Korakis. On Using Hyperledger Fabric Over Networks: Ordering Phase Improvements. In *Proc. of IEEE ICC Workshops*, 2023.

[4] Marius Corici, Pousali Chakraborty, Thomas Magedanz, Andre S. Gomes, Luis Cordeiro, and Kashif Mahmood. 5G Non-Public-Networks (NPN) Roaming Architecture. In *Proc. of NoF*, 2021.

[5] Lucas Baleeiro Dominato, Henrique Carvalho de Resende, Cristiano Bonato Both, Johann M. Marquez-Barja, Bruno O. Silvestre, and Kleber V. Cardoso. Tutorial on communication between access networks and the 5G core, 2021.

[6] Babak Mafakheri, Tejas Subramanya, Leonardo Goratti, and Roberto Riggio. Blockchain-based Infrastructure Sharing in 5G Small Cell Networks. In *Proc. of CNSM*, 2018.

[7] Bidisha Goswami and Hiten Choudhury. A Blockchain-Based Authentication Scheme for 5G-Enabled IoT. *Journal of Network and Systems Management*, 30, July 2022.