Securing E-Health Networks by applying Network Slicing and Blockchain Techniques

João Paulo de Brito Gonçalves*, Henrique Carvalho de Resende*, Esteban Municio*,
Rodolfo Villaça†, Johann M. Marquez-Barja*
*IDLab—Department of Applied Engineering, University of Antwerp—IMEC, Antwerp, Belgium
{joaopaulo.britogoncalves,henrique.carvalhoderesende,esteban.municio,johann.marquez-barja}@uantwerpen.be
†Federal University of Espirito Santo - PPGI, Vitoria - ES - Brazil
rodolfo.villaca@ufes.br

***Abstract*—Network slicing is the 5G research field that addresses the services requirements compliance over the same network. In order to robustly and securely manage the different slices in a network, we propose to use blockchain, a distributed structure that stores data without the need of an external entity to ensure data integrity and reliability. In this paper, we present a proposal on deploying a network slicing solution for Non-Public Networks (NPNs) in health environments using blockchain technology. Our solution aims to provide both performance isolation over wireless networks and privacy.**

***Index Terms*—network slicing, blockchain, security**

I. Introduction

The 3rd Generation Partnership Project (3GPP) [1] classifies the future 5G networks in two types: Public Land Mobile Networks (PLMNs) and Non-Public Networks (NPNs). The first type is the network provided directly by the Mobile Network Operator (MNO) infrastructure and will be able to address many service requisites. The second type are networks deployed for private reasons, such the ones created for indoor connectivity of sensors, robots, auto-guided vehicles, remote workers, IoT devices, wearable devices, etc.

Hospitals networks are one example of NPNs, because these networks are the medium to transmit in-site, highly sensitive information every day. Even more, to provide connectivity to in-site sensors and health services, hospitals will need to deploy or enhance the existing private network within their infrastructure. This private infrastructure will enable hospitals to prioritize network traffic and secure the information from the very edge of the network. In an European context, the use of a NPN is also mandatory in the hospitals' case because these e-health networks must comply with the General Data Protection Regulation (GDPR) [2].

Network slicing is the research topic that studies techniques to share resources and provide the expected Quality of Service (QoS) for connected clients [3]. A network slice can be defined as an expected network behavior for a specific service. In order to provide secure and distributed management of such network slicing techniques, the use of blockchain technologies can be considered as a promising approach to several use cases. Thus, in this paper we propose a network slicing solution using blockchain technology for Non-Public Networks (NPNs) hospital environments. The solution integrates state-of-the-art technologies in order to provide performance and privacy isolation in a hospital network and also an API that maintains the infrastructure synchronized with the QoS rules. Thereby, our main contributions are: (*i*) to design an architecture for network slicing in hospital environments using blockchain technology, (*ii*) to provide an prototype and instructions for network slicing in hospital environments.

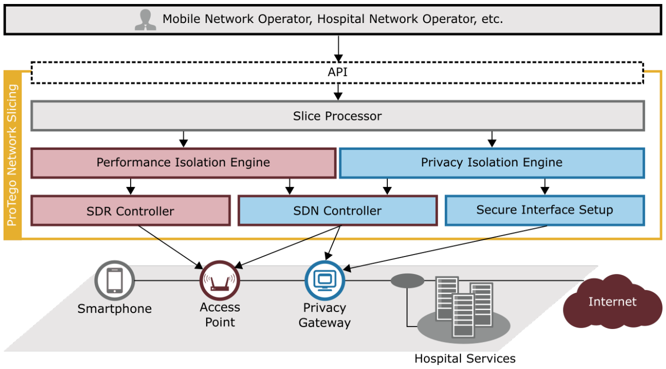

Fig. 1: ProTego's Network Slicing architecture

II. Background

A. Blockchain

The blockchain is a distributed ledger, where each participant has a copy of the database with all the validated information. Besides, a consensus protocol is implemented among the participants in order to allow them to agree about the global state of the blockchain. In a blockchain, each block is a set of transactions chained through hash addresses. In public blockchains, i.e., where access is not controlled by a central authority, validation of transactions and blocks is often based on the Proof of Work (PoW) consensus protocol. In this protocol, a cryptic challenge is proposed in order to create a valid block, once solved, the block is propagated over the network.

Several blockchain platforms have emerged in recent years and among the most popular are those based on the Ethereum platform [4]. Ethereum is a public platform for executing blockchain applications that are modeled as smart contracts and has its own cryptocurrency, the ether. It is also a very flexible alternative to the development of dApps (Decentralized Applications). A dApp uses a smart contract in the blockchain as back-end, and a web interface as front-end, allowing users to insert and receive data from the blockchain in a friendly way.

B. *Protego's Network Slicing*

ProTego project [1] is developing techniques to manage the network parameters and to increase hospital services quality using network slicing. These techniques should provide differentiation of hospital services over a wireless network, the most common type of indoor network access and should provide strategies to isolate the services flows inside the local network.

5G-EmPOWER is an SDN framework for wireless networks that provides slicing techniques [5]. Therefore, for hospital environments, the wireless slicing feature provided by 5G-EmPOWER allows the performance isolation of different services at the radio-side.

The ProTego network slicing is composed of three layers as presented in Fig. 1. The first layer is to process input from external actuators and this input could be direct configured by insertion of network parameters or providing a template [6]. This file or commands sequel is processed by the Slice Processor and generates performance and privacy rules, which are sent to the Performance Isolation Engine and the Privacy Isolation Engine. The engines can map the requirements to API calls to the different components, *i.e.*, Software-defined Radio (SDR) controller, Software-Defined Networking (SDN) controller, and the Secure Interface Setup. The SDR controller is responsible for configuring the wireless parameters and priority queues to achieve the necessary performance for the specified service. It will set the available SDN network to redirect the traffic securely and without performance degradation inside the hospital network. The Secure Interface Setup provides secure network interfaces with encryption techniques to enable the confidentiality of private data. These secure network interfaces will be available for the SDN switches to redirect the critical service flow through them and perform an extra and custom security layer for hospital services.

III. Blockchain Applied to ProTego Network Slicing

The assignment of network resources to tenants requires the resource allocation process to evolve dynamically following tenant demand variations. At the same time, the chain of network resource loans must be negotiated in a secure, transparent and fast way such that the lifecycle of each slice is not affected. Due to its decentralized nature, the blockchain technology suits well these requirements as a secure, robust and transparent management solution. The distributed ledger allows all members of the system to be aware of the current (and past) network resource availability [7].

The greatest benefits that would be achieved by applying blockchain in network slicing are:

- Secure, dynamic, and distributed consensus on network management issues.
- Reliable ledge for forensic security analysis.

Within the Protego network slicing approach, we identify slice logging as an interesting use case for blockchain. By storing and logging several slicing metrics, network slices can be securely managed and audited, ensuring higher reliability to the control plane. This may avoid malicious users to manipulate the QoS parameters to gain access to secured slices.

Due to the cost of storing data on the blockchain, log reports can be saved in some hash-based distributed file system, such as Interplanetary File System (IPFS) [8]. It is worth to mention that we do not store confidential data about health status of patients on the blockchain, only technical data related to slices updates.

IV. Conclusions and Future Work

This paper presents research on NPNs solutions focused on slice characteristics for hospital environments. A simplified NPN architecture to base the studies on experimental network slicing using the blockchain technology was presented in this paper. We will derive the most interesting approaches and will deploy one (or more) proof-of-concept to assess its feasibility.

Acknowledgements

This research has received funding from the European Union's Horizon 2020 Research and innovation program under grant agreement No. 826284 (Protego).

References

[1] 3GPP, "Service requirements for the 5G system," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 22.261, 12 2019, version 16.10.0. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107

[2] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017. [Online]. Available: https://doi.org/10.1007/978-3-319-57959-7

[3] A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5g network slicing using sdn and nfv: A survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, 2020. [Online]. Available: https://doi.org/10.1016/j.comnet.2019.106984

[4] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, 2014.

[5] S. Networks and S. S. R. U. at FBK. (2020, march) 5g-empower. [Online]. Available: https://5g-empower.io/

[6] G. Association. From vertical industry requirements to network slice characteristics. [Online]. Available: https://www.gsma.com/futurenetworks/wp-content/uploads/2018/09/5G-Network-Slicing-Report-From-Vertical-Industry-Requirements-to-Network-Slice-Characteristics.pdf

[7] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "Nsbchain: A secure blockchain framework for network slicing brokerage," *arXiv preprint arXiv:2003.07748*, 2020.

[8] J. Benet, "Ipfs-content addressed, versioned, p2p file system (draft 3)," *arXiv preprint arXiv:1407.3561*, 2014.

[1] https://protego-project.eu/