Leveraging on Network Slicing to Enable and Enhance IoT-based e-Health services

ESMERALDA BËRDUFI, University of Antwerp - imec, IDLab - Faculty of Applied Engineering, Belgium
NINA SLAMNIK-KRIJEŠTORAC, University of Antwerp - imec, IDLab - Faculty of Applied Engineering, Belgium
JOHANN MARQUEZ-BARJA, University of Antwerp - imec, IDLab - Faculty of Applied Engineering, Belgium

Network slicing plays a key role in supporting the influx of smart devices and ensuring their connectivity, because it divides the network into different logical slices over the same shared infrastructure with the aim to guaranty Quality of Service (QoS), security and isolation, which are some of the challenges that IoT systems face. The aim of this paper is to research the possibilities using Network Slicing (NS) towards enabling healthcare services with secured data flows from smart devices to cloud and then back to end user, assuring security, isolation and the required levels of QoS. In this paper, we present the study of: i) isolation and security of network slices, which is important due to interference that occur between slices and can effect the data privacy, ii) service requirements, such as e.g., latency requirement for healthcare services, which is important to have an efficient diagnosis and rapid decisions in case of any risk, and iii) building a hybrid network slicing system, combining different technologies and applying slicing, which could bring the optimal solution for end-to-end for smart healthcare and smart living.

CCS Concepts: • **Networks** → **Mobile networks**; **Wireless local area networks**.

Additional Key Words and Phrases: Internet of Things (IoT), Network Slicing (NS), logical slices, Quality of Service (QoS), WiFi

ACM Reference Format:
Esmeralda Bërdufi, Nina Slamnik-Kriještorac, and Johann Marquez-Barja. 2022. Leveraging on Network Slicing to Enable and Enhance IoT-based e-Health services. In *Conference on Information Technology for Social Good (GoodIT'22), September 7–9, 2022, Limassol, Cyprus.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3524458.3548490

1 INTRODUCTION

The Internet of Things (IoT) technology is the field that has gained the attention of different businesses and also of citizens, as the increasing number of smart devices is enabling the real-time services that are aiming to improve safety and quality of life. There are several benefits from the use of IoT in different areas of life, like healthcare- to enable fast and agile responses, smart home- remote control, industrial- to automate systems, Unmanned Aerial Vehicle (UAV)- to collect data for security and safety, energy grid - to enable smart production and distribution, smart city - to collect and share information with the public etc. As IoT technology is a wide area and involves a wide variety of different devices with different technology requirements, we are focused in two use cases, e-health and smart home. The main idea in IoT services is that the data collected in a secured way from the wearable devices or any smart device can be used in e-health to make general analysis without revelling the identity or any private information about the health of citizens, i.e., how many people did exercise, how many had potential risk in heart attack, how many do experience low or high levels of stress, in different intervals of times. According to those answers, municipalities can take action to help and encourage their citizens to live a better life.

The e-health network slicing can also be implemented in private networks as hospital network, for monitoring the patients that need fast and agile response from the medical staff. In some cases latency even in seconds can be determinant for the life of a patient. Having a dedicated slice for high risk patient monitoring will improve the effectiveness of interactions between patient and medical staff. There are different initiative taken by the European Commission for health care which include IoT technology and use of safe and protected health data [6][7]. There are also different European reports and publications about e-health services [3].

In smart home, one component can be the surveillance cameras/safe alarm, or energy consumption detector, which can send an alarm to the house owners if they have forgotten any energy consumption appliance on, and then they can, remotely, turn it off and save energy. The focus of this paper is to study the relevant technologies and research directions when it comes to applying network slicing concept to IoT use cases such as smart home and e-health, thereby trying to improve their quality of service and at the same time ensure security of data. The Network Slice (NS) is one of the promising solutions to arrange and manage IoT massive devices connectivity in private or public networks. Slicing in IoT technology means that different IoT services are assigned with different resources according to their different requirements in connectivity and security, as example: I) Some of the most relevant IoT service requirements for e-health, automotive, and transport and logistics services, are low latency and ultra-reliability, where network operators schedule transfer of data with minimal latency, e.g., remote healthcare, smart grids, intelligent transport systems, II) Supporting massive machine type services, requires to handle and differentiate traffic coming from millions of different devices. There is need to manage and control efficiently thousands of concurrent network devices to access the same network at the same time, III) Certain IoT services (e.g., video surveillance in urban traffic) require broadband communications with high transmissions rates, when devices are transmitting their information (data) simultaneously fast over time. These services have high bandwidth requirements and the traffic should be handled efficiently.

This why NS makes possible arranging and slicing the network efficiently into logical slicing fulfilling a diverse set of requirements and ensuring the required levels of Quality of Service (QoS). In the Figure 1 we show the network slice types for three general IoT use cases: I) Massive Machine Type Communication (mMTC) services: high density of devices, stable communication, long range transmission, II) Enhanced Mobile Broadband (eMBB) services: high data rate, high bandwidth, high throughput, III) Ultra-Reliable Low Latency Communication (uRLLC) services: ultra-reliable, low latency, ultra-responsive and reliable connections [23].

One of the main goals of our research is to define the service requirements in our two use cases, and based on such requirements to define the required categories of network slices that we need to create. I.e., to find out what is the required range of high bandwidth in eMBB services for IoT use cases, or the value of low latency in uRLLC for e-health, or the importance of slicing. This are some of the points that in our study we will try to answer. As it can be seen in the Figure 1, our two use cases do not fall solely in any of the corners of the triangle, they are positioned between two different corners. Smart home is between eMBB and mMTC, but closer to the first one, as for this use case we do not have very large number of devices, but we have high data and so we need high bandwidth. On the other hand, smart healthcare is closer to uRLLC than mMTC, as for remote health control we need low latency, high reliability and many wearable devices. Thus, to create a network slice for each use case we need to made a trade of between different requirements. There are different technologies that can be the solution for IoT services. Our approach is to examine which of these communication technologies can assure the network slicing that meets the requirements from each of our use cases, and make the difference between them in network slicing. Technologies like WiFi[10], 5G[22], 6G and

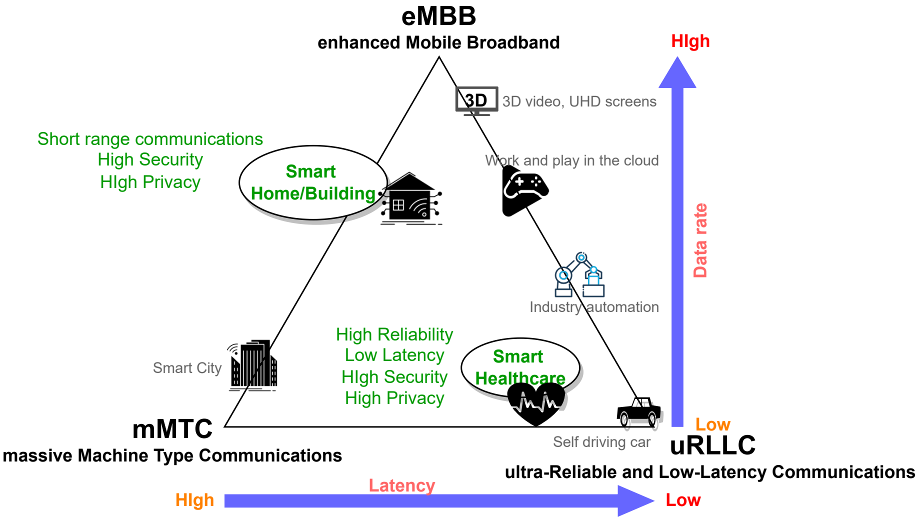

Fig. 1. Types of network slices.

beyond[15] and Block Chain are being study related to network slicing techniques. Creating slices in the air interface in all these wireless technology faces interference of massive numbers of data collecting sensors, wearable devices, smart devices, which is effecting slice isolation and security. Therefore the main comparative features are isolation and security.

We investigate on the most suitable approaches to enable secured network slices, finding the tradeoff between flexibility and scalability. Most importantly, guaranteeing the isolation among network slices and providing a secured and isolated virtual network that will transmit the data. IoT devices in smart homes or wearable devices in healthcare use cases are generally resource-constraint, that is why they are highly vulnerable to attacks. An attacker can control/dictate easily IoT devices and can force them to generate Distributed Denial-of-Service (DDoS) attacks to the network. The impact of these attacks can be minimized via isolation of IoT applications using network slicing. Moreover, dynamic allocation of idle resources to the attacked network slice is possible to keep the service without any deterioration [22].

The main challenge of network slicing is to guarantee isolation among the different network slices, i.e., logical virtual private networks that share common physical components. In this research, we aim to add mechanisms that control the isolation of the slice from data collection, e.g., sensors, to data storage and management policies. To deliver an appropriate NS we need to ensure the slice properties as: isolation, assurance, scalability, reusability. Any malicious attempt to attack the slice in healthcare or smart home can interfere in various ways, e.g., it can affect only one slice, but in absence of isolation, the slices impact each other's performance, decreasing the QoS. Network slices should be equipped with scalability so the slices can grow and shrink their instances when needed. The mechanisms that ensure dynamic management of slices, i.e., to reuse the resources previously allocated by the recently decommissioned/terminated slice, need to be ensured as well. Existing wireless slicing solutions are based on scheduling or time multiplexing (with no isolation). Our main challenge within our study is to enable slicing (with properties above) also for the IoT constrained devices, which are the devices that will be used in our use cases. We cover the range of the value chain from the data collection devices themselves (smart home devices, or wearable devices) to the network providers that transport the data, to the cloud infrastructure and service providers, to the data marketplace providers and the end customers.

In this study, we investigate different technologies embracing network slicing as a solution for smart home and smart healthcare, considering the constrained devices these two use cases use, and emphasize which communication technology can be used for serving the communication needs backed by network slicing. Our first goal in this paper is to distinguish whether using only one technology in the slice provides better support for our use cases, or combination of different technologies in different parts of slice path can meet/fulfill best the critical requirement of them. Furthermore, as a second goal, we investigate isolation and privacy aspects in network slicing for e-health and smart home, as data obtained in these use cases is sensitive to privacy and security, thereby trying to highlight the challenges and possible solutions. The last point we will cover in this study, i.e., our third goal, is the application of network slicing in uplink and downlink. As in our two use cases we have to create the slice from IoT devices to network, and these devices are connected to network via WiFi technology, we need to send data in the uplink and receive data in downlink. Based on our analysis from the state-of-the-art in WiFi slicing, we learned that the research conducted so far is mostly only considering slicing in downlink at the Access Point (AP), and there are only a few attempts in slicing WiFi in the uplink. In our approach, which is work in progress, we will try to distinguish all these challenges, pointing out from the research work what have been done until now, and what could be our focus of further research and finding solution for our two use cases, e-health and smart home.

Further more we will discuss NS in different communication technologies focusing on our eHealth and smart home use cases. Challenges and possible solutions, based on terms of, in which part of slice can these technologies be used. What are the isolation issues and if these technologies are applicable in both uplink and downlink.

2 USE CASES

As we mentioned in Section 1, the two use cases that we focus on in this paper are the e-health and smart home. The e-health promises to improve healthcare by offering new services to people and healthcare providers. Some of the services are monitoring and analysing potential risks,supporting self-management, increasing access to health care services. The e-health makes possible that citizens can access their medication profiles, can check scheduled consultations with healthcare providers, and have a history of their medication [3]. In e-health use case the idea is to have wearable devices connected to network, which send health data as heartbeat rate via network and being able to use those data to track their health risk and lifestyle, but being ensured to have secured service and data privacy. One of the most important feature for e-health care service is latency, as data are related directly to the health condition of a person, we want to be able to have a fast and agile response in case of the health risks. Some of the parameters for these features are shown in Table 1.

Smart home is one of the use cases that has gained significant attention among people, as it has a direct impact in their daily life. Requests of people on home safety, wellness/health, auto-pilot are focus of smart home technologies. We all want to be able to have a remote impact in different aspects of our homes. For smart home use case we have sensors that are connected to doors and light bulbs and also different appliance sensors. Each of these IoT devices collects sensor data and sends it to the network, and we need to take care that these data are private and secured. The consumer IoT sector has grown very fast in recent years and is forecast to continue to do so in the next years. It is expected to be more than eight billion consumers in internet worldwide by 2030 [19][18]. The use of other smart device types is still low: in 2020, only 10% of individuals in the EU used a smart thermostat, lighting solution or other smart solution for energy management in their home and even less people used smart security solutions and smart home appliances (5% of individuals) [8][18]. Smart home segment in Europe is forecast to more than double between 2020 and 2025 [20]. The main concern of citizens is the security and privacy of their data. In 2020, 13% of individuals in the

EU cited concerns about the privacy and protection of personal data generated by IoT devices or systems[8]. Therefore we put a huge effort to consider security and privacy as one of the main requirements for these use cases. The main requirement in network prospective for this use case is high data rate. As the data collected from considerable number of these devices is high in periods of time they send data simultaneously, we need to achieve high data rates so the data can be transmitted fast and in time.

3 NETWORK SLICING PHASES AND ISOLATION ISSUES

The concept of NS in any wireless communication technology, has two phases: creation phase and runtime phase. The creation phase includes Network Slice record description, service ordering, admission control, but still this phase is an open issue for further research. Runtime phase is a phase when optimization and resource reservation, Network Slice preparation and isolation occur. Each slice in network slicing is treated as an independent end-to-end network and can be assigned to particular tenants that control physical, virtualized, and service layers, which have Key Performance Indicator (KPI), such as latency, data security, energy, efficiency, mobility, massive connectivity, reachability, QoS, and throughput. The isolation constraints are set/addressed by KPIs of each slice. Wireless technology instances used to secure isolation are Management Plane and Control Plane. According to Ordonez-Lucena et al. [14], each instance has its own management plane, used to preserve management isolation. This plane consists of four functional blocks: VNF Manager (VNFM), NS orchestrator, tenant Software Defined Networking (SDN) Controller, NSL Manager.

4 WIFI NETWORK SLICING

WiFi technology is the technology mostly used worldwide to connect devices with services or other devices via the network. As IoT devices per km have reached a high number that is expected to even grow more in the coming years, we face different challenges in communication. The first one is the interference between the devices that connect at the same time with network, expected to reach one million devices/ km^2 [5]. Network slicing in WiFi enables connection of massive devices simultaneously into different services with different requirements, reaching the best use of the network. Whenever the network slices share the same network resources without reducing the performance, we may say that we have achieved network slice isolation. The second challenge is Inefficient use of allocated bandwidth, it means that bandwidth allocated to these devices is sometime wasted. There are two types/models of NS in WiFi: AP Slicing, the slice that takes place in Access Point, and Quality of Service Slicing (QoSS) and in the following sections, we detail more about both.

4.1 AP Slicing

The concept of AP Slicing applies slicing on the level of WiFi APs, considering the transmission time/airtime as a shared resource. Traffic queuing and airtime scheduling techniques are the proposed techniques to divide the AP airtime and assign it to the different slices. There are several researches and approaches in AP Slicing. The first one is Infrastructure Sharing Slice (ISS), which uses Proportional Time-Deficit Round Robin (PT-DRR) technique and Airtime Deficit Weighted Round Robin (ADWRR) technique. The PT-DRR technique counts the airtime instead of bytes, and decreases packets until the deficit reaches the value of zero, meaning that each slice asks for a specific percentage of the total airtime in AP, if there are available resources (airtime slotes) the airtime is allocated to network slice [17]. The ADWRR technique uses traffic rule by giving a relative priority. This technique is seen in Lasagna [1] framework.

[1] Lasagna: end–to–end solution that enables flexible management of slices both the wired and the wireless segments of an Enterprise wireless local area networks (WLAN). https://bit.ly/3zpRe6C

This framework pursues three objectives, programmability, isolation, and customization. Lasagna is implemented and tested in 5G–EmPOWER [2] Software–Defined Radio Access Network platform. To enable performance isolation between slices in the Lasagna framework is proposed to implement a flexible programmable hypervisor whose duty is to create, monitor, and manage network slices, considering slice isolation [17] [4].

One of the state-of-the-art approaches in AP Slicing is WiFi Service Set Identifiers (SSID) Network Slicing. In this technique, a WiFi AP provides different services to associated Stations (STA)s in an indoor environment. It means that each radio channels has different characteristics. In this case, in addition to the downlink, the uplink is also considered. WiFi SSID Network Slicing branches out in 2 algorithms, Static Slicing Algorithm and Dynamic Slicing Algorithm. In both algorithms, they take into account the Guard Interval (GI) between slices. As the GI values get increased, interference values go down, which means that isolation performance is better, but at the expense of latency values that get increased. When they increased Modulation and Coding Scheme (MCS) index, the throughput increases also, but Signal-to-Noise Ratio (SNR) decreases. The static Slicing algorithm sees the radio channels as a separated network with a distinct identifier. All slices have fixed values of GIs and MCS indexes. Dynamic Slicing algorithm is assigning to each slice a channel, updated at a run time, at an interval of time T, adapting slice performance to the network's needs, and having different algorithms for each slice type. Further research is suggested in dynamic slicing algorithm as Orthogonal Frequency Division Multiplexing (OFDMA) and Multi-User Multiple-Input and Multiple-Output (Mu-MIMO) antennas are not considered in this research [13].

4.2 QoS Slicing

As we mentioned before, network slices applied to wireless communications have to coexist within the same wireless infrastructure (e.g., healthcare data, sensor monitoring, voice over IP, video on demand). Use case slices have different and dynamic requirements in terms of performance (e.g., bitrate, latency, and reliability) that is why service-oriented approaches for network resource provisioning are needed. To answer these needs/demands, an SDN-based approach and an algorithm for on-the-fly End-to-End (E2E) QoS slice orchestration is proposed by Isolani at al. [11]. The main idea in this proposed algorithm lies in creating and adjusting the resources on APs, which are allocated for each network slice instantiated. Each slice is designed according to specific QoS requirement that a service, application, or STA needs/requires. They consider two types of slices: QoS and Best Effort (BE) slices. The QoS slice is the one where outputs need to be optimized, and BE slice is the one that can be adjusted if QoS slice face performance degradation compromised. The idea is to have many different network services that share the same infrastructure (slices) but have different QoS requirements, such as those specified by low-latency QoS, and BE modes [11].

QoS Slicing model has two main slicing techniques approaches. The first one is a proposed architecture in WLANs in Enterprise Networks where different QoS requirements are assigned to different slices. Components of this architecture are IoT Platform, IoT Broker and Wi-Fi Network Manager (WNM) and Monitor, Analyse, Plan, Execute (MAPE) loop paradigm [9]. Enterprise Networks consist of physical and virtual networks and protocols that save the dual purpose connecting all users and systems on a local area network to applications in the data center and cloud. The objective of this approach is also to define network slicing based on QoS requirement. As tests are done in simulation the interference is not included in calculation, so further reaserches can be done in base of isolation in the same approach but in real-life testbeds [9].

[2] 5G-EmPOWER: is a near-Real time Radio Access Network (RAN) Intelligent Controller for Heterogenous Radio Access Networks. https://bit.ly/3mysxxz

The second one state-of-the-art approach to AP Slicing based on QoSS is a dynamic resource allocation mechanism, which supports the development of network slicing in WiFi AP. In this QoS Slicing model, the isolation between slices is realized by defining a resource limit that a slice can use. Meanwhile, the theory of Lyapunov Optimization is applied enabling defining slices with diverse QoS requirements. This proposed solution also considers slicing the airtime as a shared resource at AP. Lyapunov optimization use Lyapunov function to control a dynamical system. They are used to provide/arrange different forms of system stability [12]. Adaptive Time-Excess Round Robin (ATERR) airtime-allocation scheduler is one of the main enablers which is modified so to be able to use the same fixed quantum size for every client. The drawback of this approach is the isolation violation due to the excess of the offered load, which means that a client exceeds the agreed max bit rate, which cause a lack of resources, i.e., fewer resources available than needed. A mechanism for guarantying isolation in this work suggests two solutions for these two particular isolation problems we just mentioned, wich are the traffic shaping (controlling and limiting the traffic to achieve parameters in the corresponding slice. agreement) and Enforcing isolation (a limit of number of resources that a slice can use) [16]. The excess of offered load means that a client exceeds the agreed max bit rate, but traffic shaping can help solve this problem. Additionally, to be able to detect and fix the isolation violation two different stages are suggested: a monitoring stage, where isolation violations are detected and monitored, and an action stage, where actions are done to fix the violations and move the system to a stable state [12]. All these solutions in QoS Slicing WiFi AP have been shown to define slices with different QoS requirements and also provide slice isolation. However, the results are mostly acquired only from the simulation environments, and have to be also collected and tested in real-life testbeds.

5 5G AND 6G NETWORK SLICING

Network Slicing is defined as main enabling technology in 5G and 6G networks. As regards to different use cases and requirements, network slices are separated in three main slice types as shown above in the Figure 1. The three main slices are: eMBB, mMTC, uRLLC, while in 6G there is an extended definition to i) Extreme URLLC (eURLLC), ii) Further eMBB (FeMBB), iii) Ultra mMTC (umMTC), iv) Long Distance and High Mobility Communications (LDHMC) for deep see sightseeing and space travel, and v) Extremely Low-Power Communications (ELPC) to enable e-health and nano robots. In Figure 1 are also shown the parameters for each slice type, and our two use cases are placed somewhere between the corners of the triangle. For our e-health use case we can not be in the corner of the triangle, i.e., uRLLC as we need combination of parameters between mMTC slice and uRLLC slice. Based on the specific e-health use case trade of between parameters can be done. In 5G network architecture slicing can take place in three different sections, so the slice techniques are named base on the place they are: RAN Slice Network, Transport Slice Network and Core Slice Subnet. More researches are done about slicing RAN network, and slices in RAN network can be shared or non-shared slices. Similarly, in 6G architecture, slicing can take place in three different layers, so the slice techniques are named based on architecture layers: Intelligent Cloud Slicing Layer, RAN Slicing Layer, Application Slicing Layer.

Each slice has a lifecycle it goes through, which is composed of four phases: Preparation, Creation, Operation and Termination [2]. The requirements that 5G aims to achieve using NS are shown in Table 1. Medical health systems will also benefit from the 6G wireless systems due to innovations, such as AR/VR, holographic telepresence, mobile edge computing, and Artificial Intelligence (AI), which are the cornerstone of future smart healthcare systems [15]. A reliable remote monitoring system in the healthcare system will be facilitated by the 6G systems. Even remote surgery will be made possible by using 6G communication. A high data-rate, low latency, and ultra-reliable 6G network will help to quickly and reliably transport huge volumes of medical data, which can improve both the access to care and the quality of care.

Table 1. Comparison: 5G vs 6G vs WiFi 6 Network Slice.

	Area Traffic Capacity ($Mbps/m^2$)	**Connection Density** ($devices/km^2$)	**Peak Data Rate** ($Gbps$)	**Cell Edge /Data Rate per User Rate** ($Mbps$)	**RAN Latency** (ms)	**Channel bandwidth** (MHz)
5G	10	10^6	DL: 20, UL: 10	DL: 100, UL: 50	< 1	20, 40, 80, 100
6G	1000	10^7	DL:1000 − 10000, UL: 1000	DL: 10000, UL: > 1000	< 0.1	N/A
WiFi 6	N/A	inside: $> 80m$ outside: $> 300m$	DL: 9.6, UL: 5	100	< 20	20, 40, 80, 160
Smart home	N/A	25 IoT devices/home	0.01	N/A	N/A	N/A
e-health	N/A	N/A	0.1	N/A	1 to 10	N/A

However, along with the growth of the networks, the challenges about security grow as well. The 5G NS security challenges are subject of ongoing studies and researches, whereas the main security principles and respective security breaches are: i) Confidentiality gets affected when attacker monitors the traffic in northbound/southbound interfaces, ii) Authentication, affected by Confidentiality breaches, iii) Authorization, affected by Confidentiality breaches, iv) Availability, happens when attacker injects traffic in the above interfaces, and v) Integrity, a compromise of any network functions may allow access to control-plane functionalities [21].

6G slicing issues include well known challenges like slice isolation, necessity for efficient dynamic slice creation and deletion, slicing RAN effectively – when is suggested slicing RAN with 2-layerd control granularity with new algorithms. Securiy Function Virtualization (SFV) for NS is a technique (simulator) suggested for security in 6G slicing, to fix Remote attestation, Network isolation Levels (trusted, vulnerable, compromised slices), blockchain with modified version: dynamic Proof of Work (dPoW) [1].

In particular, the Blockchain and Machine Learning are the breakthrough technologies in 6G and beyond that are expected to solve the IoT network model, improve security and pave the way for future massive IoT communications, but their true impact on e-health and smart home need to be further studied and addressing also to the security and privacy issues. The technologies like Blockchain /Distributed Ledger Technology (DLT), Quantum Computing, Distributed and Scalable AI/ML, Physical Layer Security (PLS) are supposed to help with security issues in general in 6G and beyond [15].

6 CONCLUSION

In this paper, we have presented our work in progress on network slicing techniques that enable and enhance smart home and e-health services. We have outlined the main approaches and motivation for such a challenging topic, recognizing the importance of selecting the optimal communication technology for network slicing in our use cases, enabling isolation between slices and fulfilling the requirement to be able to send and receive data (uplink/downlink) in each slice. Further research needs to be intensified in uplink of WiFi networks, as there is a big gap in UL slicing, it remains still challenging to create end to end uplink NS since we can not interfere/make any changes in STAs part. Another challenge is securing the slices in airtime allocation. Our paper provides a baseline for the network slicing specially in WiFi. The main goal of our future work is to design network slicing mechanisms for e-health and smart home use cases using WiFi 5 and WiFi 6, where the main requirements are isolation of the slices, privacy of the data and technical requirements for each of use cases to achieve the guaranteed levels of QoS.

ACKNOWLEDGMENTS

This work is supported by the Flemish Government through FWO SBO project MOZAIK S003321N, as well as the European Union's Horizon 2020 project VITAL-5G co-funded by the EU under grant agreement No. 101016567.

REFERENCES

[1] Muhammad Naveed Aman, Uzair Javaid, and Biplab Sikdar. 2021. Security Function Virtualization for IoT Applications in 6G Networks. *IEEE Communications Standards Magazine* 5, 3 (2021), 90–95. https://doi.org/10.1109/MCOMSTD.201.2100023

[2] GSM Association. 2021. E2E Network Slicing Architecture. *IEEE Journal on Selected Areas in Communications* (2021). https://bit.ly/3xjIbTm

[3] European Commission, Directorate-General for Health, Food Safety, F Lupiáñez-Villanueva, L Gunderson, S Vitiello, N Febrer, F Folkvord, L Chabanier, N Filali, R Hamonic, E Achard, H Couret, M Arredondo, M Cabrera, R García, L López, B Merino, and G Fico. 2022. *Study on health data, digital health and artificial intelligence in healthcare.* https://doi.org/doi/10.2875/702007

[4] Estefanía Coronado, Roberto Riggio, José Villa1ón, and Antonio Garrido. 2018. Lasagna: Programming Abstractions for End-to-End Slicing in Software-Defined WLANs. In *2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM).* 14–15. https://doi.org/10.1109/WoWMoM.2018.8449797

[5] Sabine Dahmen-Lhuissier. 2018. *ETSI - Mobile Technologies - 5g, 5g Specs | Future Technology.* https://bit.ly/3zonffu

[6] EU. 2022. *EU4Health programme 2021-2027 – a vision for a healthier European Union.* https://bit.ly/3Q2j1A2 Datatracker.ietf.org.

[7] EU. 2022. *European Health Data Space.* https://bit.ly/3Nxf7h6 Datatracker.ietf.org.

[8] Eurostat. 2020. *Number of Internet of Things (IoT) smart home devices worldwide.* https://bit.ly/3aS9awR Datatracker.ietf.org.

[9] Foroutan Fami, Chuan Pham, and Kim-Khoa Nguyen. 2020. Towards IoT Slicing for Centralized WLANs in Enterprise Networks. In *2020 International Symposium on Networks, Computers and Communications (ISNCC).* 1–6. https://doi.org/10.1109/ISNCC49221.2020.9297339

[10] Jetmir Haxhibeqiri, Pedro Heleno Isolani, Johann M. Marquez-Barja, Ingrid Moerman, and Jeroen Hoebeke. 2021. In-Band Network Monitoring Technique to Support SDN-Based Wireless Networks. *IEEE Transactions on Network and Service Management* 18, 1 (2021), 627–641. https://doi.org/10.1109/TNSM.2020.3044415

[11] Pedro Heleno Isolani, Nelson Cardona, Carlos Donato, Johann Marquez-Barja, Lisandro Zambenedetti Granville, and Steven Latré. 2019. SDN-based Slice Orchestration and MAC Management for QoS delivery in IEEE 802.11 Networks. In *2019 Sixth International Conference on Software Defined Systems (SDS).* 260–265. https://doi.org/10.1109/SDS.2019.8768642

[12] Michael Neely. 2010. *Stochastic Network Optimization with Application to Communication and Queueing Systems.* https://bit.ly/3Q4PbLq

[13] Matteo Nerini and David Palma. 2021. 5G Network Slicing for Wi-Fi Networks. In *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM).* 633–637. https://ieeexplore.ieee.org/document/9463988

[14] Jose Ordonez-Lucena, Oscar Adamuz-Hinojosa, Pablo Ameigeiras, Pablo Muñoz, Juan J. Ramos-Muñoz, Jesús Folgueira Chavarria, and Diego Lopez. 2018. The Creation Phase in Network Slicing: From a Service Order to an Operative Network Slice. In *2018 European Conference on Networks and Communications (EuCNC).* 1–36. https://doi.org/10.1109/EuCNC.2018.8443255

[15] Pawani Porambage, Gürkan Gür, Diana Pamela Moya Osorio, Madhusanka Liyanage, Andrei Gurtov, and Mika Ylianttila. 2021. The Roadmap to 6G Security and Privacy. *IEEE Open Journal of the Communications Society* 2 (2021), 1094–1122. https://doi.org/10.1109/OJCOMS.2021.3078081

[16] Matías Richart, Javier Baliosian, Joan Serrat, Juan-Luis Gorricho, and Ramón Agüero. 2020. Slicing With Guaranteed Quality of Service in WiFi Networks. *IEEE Transactions on Network and Service Management* 17, 3 (2020), 1822–1837. https://doi.org/10.1109/TNSM.2020.3005594

[17] Matías Richart, Javier Baliosian, Joan Serrati, Juan-Luis Gorricho, Ramon Agüero, and Nazim Agoulmine. 2017. Resource allocation for network slicing in WiFi access points. In *2017 13th International Conference on Network and Service Management (CNSM).* 1–4. https://doi.org/10.23919/CNSM.2017.8256046

[18] European COMMISSION STAFF. 2021. *PRELIMINARY REPORT - SECTOR INQUIRY INTO CONSUMER INTERNET OF THINGS.* https://bit.ly/3zpgMAU

[19] Statistics. 2020. *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030.* https://bit.ly/3zqldlf Datatracker.ietf.org.

[20] Statistika. 2020. *Smart Home - revenue forecast in Europe from 2017 to 2025 (in million U.S. dollars.* https://bit.ly/3xzIkkP

[21] Tomasz Wichary, Jordi Mongay Batalla, Constandinos X. Mavromoustakis, Jerzy Żurek, and George Mastorakis. 2022. Network Slicing Security Controls and Assurance for Verticals. *Electronics* 11, 2 (2022). https://doi.org/10.3390/electronics11020222

[22] Shalitha Wijethilaka and Madhusanka Liyanage. 2021. Survey on Network Slicing for Internet of Things Realization in 5G Networks. *IEEE Communications Surveys & Tutorials* 23, 2 (2021), 957–994. https://doi.org/10.1109/COMST.2021.3067807

[23] Fanqin Zhou, Peng Yu, Lei Feng, Xuesong Qiu, Zhili Wang, Luoming Meng, Michel Kadoch, Liang Gong, and Xianjiong Yao. 2020. Automatic Network Slicing for IoT in Smart City. *IEEE Wireless Communications* 27, 6 (2020), 108–115. https://doi.org/10.1109/MWC.001.2000069