AI-driven Zero-touch Operations, Security and Trust in Multi-operator 5G Networks: a Conceptual Architecture

Gino Carrozzo[+], M. Shuaib Siddiqui[++], August Betzler[++], José Bonnet[+++], Gregorio Martinez Perez[*], Aurora Ramos[**], and Tejas Subramanya[***]
[+] Nextworks, Pisa, Italy; [++] i2CAT Foundation, Barcelona, Spain; [+++] Altice Labs, Aveiro, Portugal;
[*] Univ. Murcia, Murcia, Spain; [**] ATOS, Madrid, Spain; [***] Fondazione Bruno Kessler, Trento, Italy;
Corresponding author: Gino Carrozzo, g.carrozzo@nextworks.it

***Abstract*— The 5G network solutions currently standardised and deployed do not yet enable the full potential of pervasive networking and computing envisioned in 5G initial visions: network services and slices with different QoS profiles do not span multiple operators; security, trust and automation is limited. The evolution of 5G towards a truly production-level stage needs to heavily rely on automated end-to-end network operations, use of distributed Artificial Intelligence (AI) for cognitive network orchestration and management and minimal manual interventions (zero-touch automation). All these elements are key to implement highly pervasive network infrastructures. Moreover, Distributed Ledger Technologies (DLT) can be adopted to implement distributed security and trust through Smart Contracts among multiple non-trusted parties. In this paper, we propose an initial concept of a zero-touch security and trust architecture for ubiquitous computing and connectivity in 5G networks. Our architecture aims at cross-domain security & trust orchestration mechanisms by coupling DLTs with AI-driven operations and service lifecycle automation in multi-tenant and multi-stakeholder environments. Three representative use cases are identified through which we will validate the work which will be validated in the test facilities at 5GBarcelona and 5TONIC/Madrid.**

***Index Terms*— 5G, Zero Touch Automation, Spectrum Sharing, Artificial Intelligence, Distributed Ledger Technologies**

I. Introduction

It is commonly recognised that 5G is one of the main catalysts for the digitalisation of our society: ultra-high bandwidth, low latency and increased connectivity density are some of its main characteristics. Despite the progress in the development of 5G technologies and standards, 5G networks nowadays are not yet at the stage of complete achievement of all the performance requirements and features initially envisioned. In fact, 5G deployments today are occurring at limited scale and most of the current releases target enhanced Mobile Broadband (eMBB) services with 5G New Radio (5G NR), but still they do not allow coexistence of different types of vertical applications (i.e. eMBB with Ultra-Reliable Low-Latency Communications -URLLC- and/or with massive Machine Type Communications -mMTC). Moreover, network slicing specified by 3GPP and network monitoring with analytics are not fully supported and do not span multiple operator domains.

In view of a 5G evolution, apart from working for the full achievement of the performance KPIs for the different service categories, it is needed also to incorporate more disruptive approaches and technologies for resource and spectrum sharing, network orchestration, end-to-end security and trust. For this, three novel design principles are emerging in the technical community working on 5G. First, Artificial Intelligence (AI) can transform network management into a cognitive process through which the network can self-adapt and self-react to changing conditions with minimal manual intervention (zero-touch). Second, Distributed Ledger Technologies (DLT)/Blockchains (BC) can be adopted to implement distributed security and trust across the various parties involved in the 5G service chain. Third, Cloud Native technologies can allow to achieve the necessary level of flexibility, scalability and resilience of SDN/NFV-based services for 5G. It is our vision that these three technologies, coupled with the advancement of the 5G specifications at 3GPP, can ensure the needed efficient delivery of cutting-edge 5G services.

Moreover, there is a need to overcome the bilateral B2B models traditionally adopted by operators, which currently only implement sharing of passive infrastructure and roaming. We envision that a multi-party distributed model is needed to develop a profitable business in 5G through which a large group of parties, from Telcos to Verticals and spectrum owners, can establish cross-domain service chains with security and trust.

The H2020 5GZORRO project [1], a 5G PPP Phase 3 research project, has been recently launched to specifically address all these aspects.

The remainder of this paper is organized as follows: Section II highlights the main challenges we envision for 5G evolution; Section III introduces the 5GZORRO platform conceptual architecture and the use cases that will be used to validate its main characteristics; finally, Section IV draws some conclusions by gives insights on future development work and validation plans.

II. Main Challenges towards 5G Evolution

Up to nowadays, security and zero-touch automation aspects have been addressed as distinct parts of network and service management, leading to non-integrated solutions. To ensure reliable and secure communications in 5G, the need for joint realization of zero-touch security and trust framework is emerging.

We identified three main challenges for 5G evolution which technologies like AI-driven orchestrations, DLTs and

zero touch automation can help to solve in distributed, heterogeneous and multi-operator 5G systems. These challenges are respectively represented as 1-blue, 2-red and 3-green circles in Fig. 1.

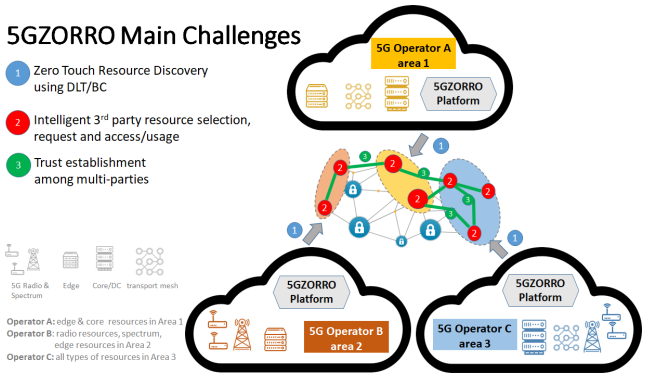

Fig. 1. Multi-party zero-touch security and trust challenges for 5GZORRO.

A. Dynamic spectrum management

Spectrum, both licensed and unlicensed, is a key asset in 5G and hence its efficient use is of paramount importance. Cellular networks (2G, 3G, 4G) are example technologies that use licensed spectrum; whereas WiFi or Bluetooth (IEEE 802.11, 802.15) are typically unlicensed spectrum.

Regulators have recently allowed requests for licensed spectrum in small local areas. Verticals are typically looking at this spectrum usage option e.g., in relation to Industry 4.0 factory automation scenarios.In such an evolving context, it might be optimal to seek spectrum sharing mechanism which include the Regulator and also Mobile Network Operators (MNO). In this case, 5G Verticals may deploy private 5G networks by using licensed spectrum which has already auctioned and then lent by a traditional MNO.

Related work in literature has just investigated how to optimize the use of spectrum in cognitive radios. The cognitive radio architecture was based on two principles: i) real-time sensing capabilities in the radios, and ii) a spectrum broker to handle radio requirements from different users. This paradigm has lately also been aligned with SDN architecture to coordinate access points operating in unlicensed spectrum in residential buildings [2]. However, cognitive radio architectures have not enjoyed a wide adoption due to the practical difficulty of realizing a spectrum broker.

In fact, a critical aspect on dynamic spectrum allocation is the coexistence of technologies that share unlicensed bands. Two models are currently discussed to incorporate cellular technologies in unlicensed spectrum. The first model consists of having cellular technologies mainly operating in licensed spectrum, but allowing to increase capacity by incorporating an additional carrier in unlicensed spectrum. The second model consists of deploying cellular technologies directly in the unlicensed band without an anchor in a licensed band, thus competing for the medium with WiFi technologies. An example of this approach is LTE-unlicensed described in [3]. An alternative approach has been proposed by FCC in the US to regulate access to spectrum in the 3.5 GHZ band, which is known as the Citizens Broadband Radio Service (CBRS).

Other works propose the use of Blockchains to bridge the gap that spectrum brokers in cognitive radio architectures failed to address in state of the art. In [4], the idea of a spectrum market is proposed and analysed from a theoretical perspective.

However, it remains still to be solved the problem of implementing a practical Blockchain based spectrum market, capable of securing the information that agents declare in the market.

B. Automated service and network management

5G use cases have requirements on ultra-low latency, high throughput, and connectivity density, causing networks to be transformed into softwarized, service-based, and holistically-managed infrastructures, using enablers such as NFV, SDN, and MEC. Such distributed, multi-technology, and multi-domain nature increase the complexity in the way end-to-end networks and services are managed and orchestrated, making intelligent automation via AI a dire necessity.

In recent years, we have seen an increasing demand for automating management in many areas of IT, introducing a concept called AIOps (AI for IT Operations) [5]. AIOps involves efficient data collection, storage and analytics to provide valuable insights. The AIops concept can be extended to the context of 5G networks for spectrum management, lifecycle management, and fault, configuration, accounting, performance, security (FCAPS).

Research efforts on AI-driven network management solutions are being carried out, like in SLICENET [6]. However, most of the existing solutions rely on statistical methods and basic machine learning algorithms. Furthermore, the lack of trust between marketplace participants prevents sharing the operations data openly, hindering the applicability of AI techniques to end-to-end network and service management.

In this context, it is envisioned that a common data layer could be provided for storing and processing operational data across multiple domains, parties, abstraction layers, and management functions. This data layer, called Operational Data Lake, will serve as basis for intelligent resource and service management.

In the context of operational data lakes, it is particularly interesting the possibility of training machine learning models in a distributed way (e.g., Federated Learning) without compromising on the privacy and security aspects of centralized ML algorithms. The resulting AI capabilities can be used to implement more effective 5G network and service management at large scale.

C. Cross-domain trust across multiple operators

Some of the service models and technologies introduced with 5G introduce new security risks to data, services and networks. These security risks are higher in multi-tenant and multi-stakeholder scenarios, and become particularly challenging in scenarios of critical communications. The H2020 5G PPP 5G-ENSURE [7] project just provided trust

models intending to identify different trust zones that suit the requirements of end users and network operators. The project identified different ranges of trust going from zero trust (system or network fully trustworthy) to open trust (trust cannot be guaranteed) and addressed interactions among different actors. Other research works like [8] describe the concept of Trust Zone where a Authorization and Authentication architecture is taken to the network edge, especially for emergency scenarios, enabling the application of autonomous and decentralised policies in a multi-tenant 5G scenario.

Blockchains can provide an additional level of trust to a 5G scenario. In [9] authors design a Blockchain Slice Leasing Ledger with the intention of improve service creation time and network operation efficiency. An interesting contribution in the telecommunications sector is Clear X [10], a clearing solution employing proprietary DLTs, smart contracts and zero knowledge proof protocols and tokens to enable enterprise level clearing.

The aspects of cross-domain trust have also to consider contexts of massive number of users, very low latency and higher data rates requests across high device connection densities. These new 5G scenarios can create a new-generation of hazard landscape, with new emerging vulnerabilities affecting different 5G architectural layers. In particular, at the physical layer security threats may impact hardware and wireless channels, whilst at the logical layer they could consist of data leakage over shared resources, hypervisor hijacking or NFV/SDN layer denial of service (DoS). Moreover, network slices in multi-cloud and multi-operators environments spark new security concerns, which require a high level of isolation at the management, control and resource layers to ensure network slices. Therefore, strict isolation between slices in multi-tenant cloud infrastructures is a major challenge.

A comprehensive study on 5G security challenges and solutions in clouds, SDN and NFV can be found in [11].

III. Combining zero-touch automation and distributed ledger technologies for 5G

The use of NFV, SDN and service-based architectures for implementing the 5G networks brings a radical change in network and service orchestration. Nevertheless, the introduction of 5G service elements in operational infrastructures is posing the challenge of streamlining the multiple management frameworks specifically tuned for different technologies, aiming at a uniform end-to-end 5G service management.

Current solutions for 5G networks are not yet capable to fully address this scenario and some limits exist in the possibility to extend 5G services in a truly pervasive way, with trust, security and accountability.

5GZORRO starts from necessity to evolve architectures and management solutions in truly multi-stakeholder environments where heterogeneous compute, storage and network resources along with spectrum are integrated to implement a ubiquitous service coverage across domains.

As depicted in Fig. 2, the 5GZORRO platform architecture follows a principle of service based architectures similar to the 5G Service-based architecture [12], and the ETSI Zero-touch Network and Service Management [13]. Through a Permissioned Distributed Ledger infrastructure, the platform offers services for: 1) Smart Contracts Management, 2) Resource Discovery Brokering; 3) Intelligent 3rd-party virtual resource selection; 4) Spectrum trading and sharing; 5) Secure SLA Monitoring.

Within the platform, the realization of these services is made possible through the interaction of various functions for slice orchestration, Network Intelligence and analytics, Security Trust, Management of Service virtualized Resources, all executed for multi-domain and single domain scope

The architecture implements the concept of sharing operational data across the whole system in a logically centralized data reservoir (a.k.a. Data Lake), so that multiple asynchronous management components may act upon this shared data pool towards optimizing a target set of KPIs. To facilitate open data sharing, permissioned ledgers are used for governance of and accounting for data use.

The 5G Operational Data Lake component serves as a logically centralized reservoir of all the operational data, channelled by management services of Inter-domain Layer on behalf of domain specific management services running in every domain of the Single Domain Layer. It will provide APIs for adding, processing (in place) and retrieving data for analytical processes. These APIs can be invoked by the management components in the Inter-domain Layer and by the service components in the Evolved 5G Service Layer without incurring any unneeded coupling between the data providers and the data consumers.

The 5G Permissioned Distributed Ledger component ensures the aforementioned interoperability by providing data governance, multi-party trust, and accounting for data usage by different participating parties.

A. Conceptual architecture of the 5GZORRO platform

The 5GZORRO conceptual architecture (see Fig. 2) incorporates zero-touch automation solutions to orchestrate high volumes of ubiquitous and pervasive 5G services, with security and trust. It makes use of AI to govern the complexity of the requested automation, and DLTs to implement a scalable and secure solution for the interworking of the actors of the service composition chain.

Through the 5GZORRO architecture, distributed networks and computing resources, spectrum and services capabilities from different domains and service providers can be automatically discovered and "inventorized". On these network assets discovered across multiple operator domains (see Fig. 1), intelligent 3rd-party resource selection, request and access/usage is implemented to allow:

- Efficient Day-0 operations (i.e. instantiation) across administrative domains, with (i) Seamless use of heterogeneous virtualization platforms; (ii) Use of different 5G radio spectrum from different licensed owners; (iii) On-board functions and services defined by multiple

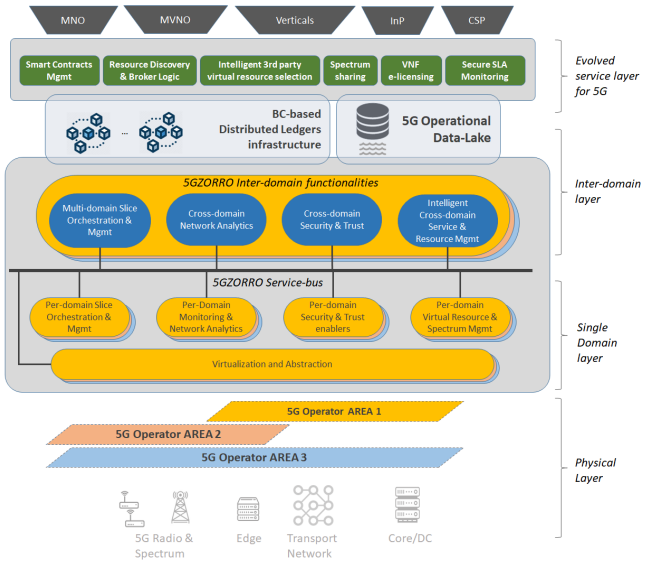

Fig. 2. Conceptual architecture of the 5GZORRO platform

providers with security and trust; (iv) Resource placement, spectrum use and service composition across domains; (v) Service Function split and related service mesh networking with efficiency with respect to KPIs.

- Intelligent Day-1 (i.e. configuration) and Day-2 (i.e. optimization) actions, leveraging on AI techniques to process the monitoring information from the service domains in order to: (i) optimize network operations; (ii) implement SLA monitoring across the multi-party service chain; (iii) maintain security, privacy and trust.
- Establish trust among the parties via Blockchain, a DLT which allows managing the complexity of a multi-stakeholder framework. Blockchain do not request trust a-priori between parties, and it can implement automated settlements by using Smart Contracts.

B. Use cases

The 5GZORRO architecture will be validated in three relevant use case environments.

(1)**Smart Contracts for Ubiquitous Computing/Connectivity**. This use case originates from the consideration that the telecommunications sector at large still relies on offline, non-standard paper contracts to establish commercial interactions, including SLAs, which is inflexible and unsuitable for real-time resource supply and demand among the multiple parties involved in 5G.

The 5GZORRO architecture can support smart contracts with a business logic of various multilateral agreements. This standardisation enables the automation of commercial, technical and SLA interactions between all parties by means of implementing a DLT environment that allows trustless interactions. All the parties will be able to verify the identity of participating nodes and its the resource contribution in relation to the end-to-end provision of services to the consumer and to other entities.

As depicted in Fig. 3, we foresee the inclusion of oracles, i.e. agents that verify real-world occurrences and submit the information to a blockchain to be used by smart contracts. Existing standards about the provision of ubiquitous computing and connectivity can be mapped into Oracle Smart Contracts for reference by inter-party Smart Contracts. New Oracle Smart Contracts containing commercially relevant data such as unit pricing (e.g. minute, MB, etc) will provide a central point of reference for ad-hoc multi-party Smart Contracts.

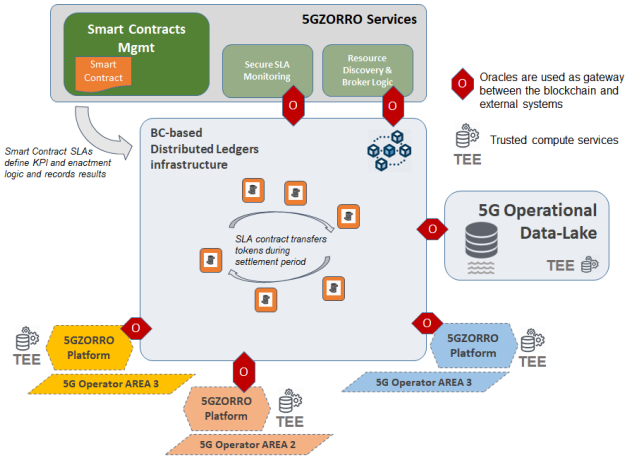

Fig. 3. Smart Contracts for Ubiquitous Computing and Connectivity Use Case.

(2) **Dynamic spectrum allocation**. 5G verticals may require licensed spectrum but only for small local areas, for example to deliver robotic automation in a factory using 5G. Given the need to avoid harmful interference, the 5G vertical cannot use unlicensed spectrum, hence it will be optimal to seek spectrum sharing mechanism including spectrum leasing from MNOs.

In 5GZORRO, we intend to use the distributed trust offered by DLT infrastructures to efficiently coordinate the sharing of spectrum and implement a dynamic and efficient 5G spectrum market. Shared spectrum right holders can trade spectrum rights for a given area and time in a spectrum market, thus enhancing spectrum efficiency while allowing QoS. This will also allow many stakeholders to participate in spectrum trading.

Fig. 4 illustrates how the envisioned spectrum market relates to the 5GZORRO architecture. A set of business agents will obtain a spectrum license issued by the regulators (point 1 in Fig. 4). The provided license would be bound to a certain geographic area and time period, which is equivalent to a set of spectrum token (spectoken). These users would then be able to exchange spectoken with each other for spectrum rights (point 2 in Fig. 4). MNOs could also participate in this market, by offering the excess spectrum that they are not using. On the demand side, an example could be a stadium that may want nearby spectrum rights during the match time.

(3) **Pervasive vCDN Services**. In a 5G network using segmented and distributed virtualized resources allocated into

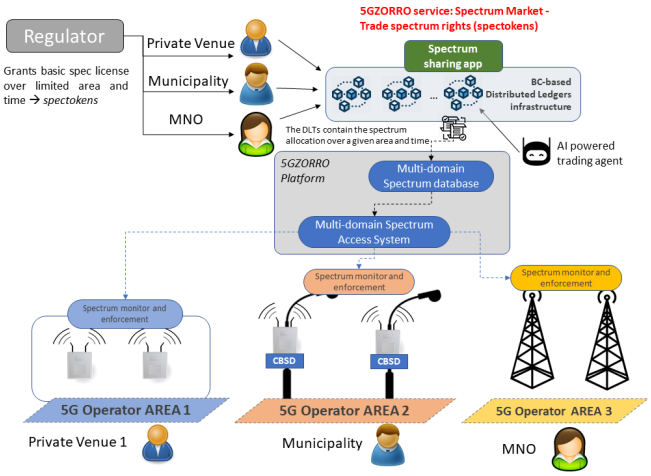

Fig. 4. 5GZORRO spectrum market scenario.

network slices, a content service provider may need to dynamically modify the deployment of its virtual functions ans services at a given place due to varying demand dynamics, typically associated with user mobility and e.g., content popularity.

The possibility to leverage on 3rd-party resources from different operators can allow to flexibly extend service coverage to various locations and compose virtualized assets from various providers into a single end-to-end network slice.

As depicted in Fig. 5, through the 5GZORRO architecture a content service provider who offers virtualized content delivery network (vCDN) services can use the resource discovery process to identify usable 3rd-party resources and the candidate target infrastructures capable of maintaining trust & security for the service, and consequently select and automatically re-instantiate its vCDN elements by optimizing target KPIs, security/trust properties, pricing, etc.

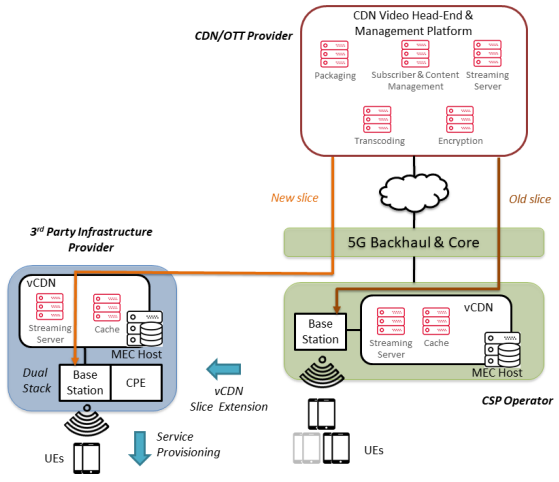

Fig. 5. Pervasive vCDN Services scenario in 5GZORRO.

As a result, a network slice extension to extend into 3rd-party 5G network infrastructures is implemented.

IV. Conclusion And Future Work

The consolidation of 5G networks passes through the implementation of multi-stakeholder scenarios in which 5G resources and services are exposed, traded and chained across multiple operators to implement the ubiquitous computing and connectivity envisaged for 5G networks.

In this paper, we presented some key challenges and a conceptual architecture for the evolution of 5G networks in multi-operator scenarios. Some related use cases are briefly described which will be used to validate the concepts of smart contracts for 5G networks, spectrum market and zero-touch automation.

This architecture is currently being specified in terms of services and interfaces within the context of the H2020 research project 5GZORRO, which is part of the 5G PPP Phase 3 - 5G long term evolution.

The 5GZORRO architecture and its corresponding platform will offer the aforementioned functionalities and AI-driven operation services. Initial prototypes of its components are planned to be validated in the testing facilities of 5GBarcelona and 5Tonic-Madrid fmo Q1-2021.

Acknowledgement

This work was funded by the European Commission through 5GZORRO project (grant no. 871533) part of the 5G PPP in Horizon 2020 programme. The paper solely reflects the views of the authors. EC is not responsible for the contents of this paper or any use made thereof. Authors thank also the entire 5GZORRO Consortium for useful insights and contributions to this work.

References

[1] 5gzorro, h2020 5g ppp project. [Online]. Available: http://www.5gzorro.eu/
[2] A. Zubow, M. Döring, M. Chwalisz, and A. Wolisz, "A sdn approach to spectrum brokerage in infrastructure-based cognitive radio networks," in *2015 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, Sep. 2015, pp. 375–384.
[3] W. M. C. L. X. Z. Z. S. X. . X. L. L. Zhang, R., "Lte-unlicensed: the future of spectrum aggregation for cellular networks," in *IEEE Wireless Communications 22(3)*. IEEE, 2015, pp. 150–159.
[4] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 32–39, March 2018.
[5] Artificial intelligence for it operations. [Online]. Available: https://www.ibm.com/cloud/aiops/
[6] Slicenet, h2020 5g ppp project. [Online]. Available: https://slicenet.eu/
[7] 5g-ensure, h2020 5g ppp project. [Online]. Available: http://www.5gensure.eu/
[8] B. Han, S. Wong, C. Mannweiler, M. Dohler, and H. D. Schotten, "Security trust zone in 5g networks," in *2017 24th International Conference on Telecommunications (ICT)*. IEEE, 2017, pp. 1–5.
[9] J. Backman, S. Yrjölä, K. Valtanen, and O. Mämmelä, "Blockchain network slice broker in 5g: Slice leasing in factory of the future use case," in *2017 Internet of Things Business Models, Users, and Networks*. IEEE, 2017, pp. 1–8.
[10] Clear x. [Online]. Available: https://www.clearx.io
[11] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, 03 2018.
[12] 5g system, technical realization of service based architecture (3gpp specification 29.500). [Online]. Available: http://tiny.cc/65hbkz
[13] Zero touch network and service management. [Online]. Available: http://tiny.cc/g5hbkz