A Survey on the Security of European 5G Private Networks

Pelin Angin[1]*, Manolya Atalay[1], Fatma Ceyda Gokce[1], and Ilsun You[2]
[1]Department of Computer Engineering, Middle East Technical University, Turkey
{pangin, manolya}@ceng.metu.edu.tr, ceyda.gokce@metu.edu.tr
[2]Department of Information Security, Cryptology, and Mathematics, Kookmin University, South Korea
ilsunu@gmail.com

Received: October 10, 2022; Accepted: December 3, 2022; Published: December 15, 2022

Abstract

The introduction of 5G networks has created opportunities for many vertical use cases through strong support for massive Internet of Things (IoT) connections with three main promises, i.e., massive machine type communications, enhanced mobile broadband and ultra-reliable low latency communications. With the enlarged network surface and the new technologies such as software-defined networking and network functions virtualization utilized to support the promised functionality, new security requirements have arisen. This paper focuses on private 5G networks and provides an overview of the security challenges they face along with a survey of approaches proposed for solving those challenges.

Keywords: 5G, Private networks, Security.

1 Introduction

The Fifth Generation Public Private Partnership (5G-PPP) foresees that in the near future, over 5 trillion devices will be connected through 5G with shortened time for service creation and additional privacy protection mechanisms [1]. Network Functions Virtualization (NFV) will be able to support the requirements of such networks through advanced portability and flexibility in wireless communication technology. One of the principal instruments for flexibility is separating the data forwarding plane and network control plane with Software Defined Networks (SDN) [2].

In the history of wireless communications, security vulnerabilities have always existed. During the 1G wireless network era, wireless channels and mobile phones were targets for many attacks, including masquerading and illegal cloning. When 2G wireless networks came into play, spam messages, including but not limited to undesired marketing and false information insertion attacks, became popular. IP-based communications within 3G networks introduced cellular devices' existing wireless network security vulnerabilities. 4G cellular networks have provided the necessary infrastructure for an unprecedented increase in intelligent devices, high-volume multimedia traffic, and new services in the cellular space.

Consequently, the threat landscape became more dynamic and complex. With the introduction of 5G wireless networks, there will be more privacy concerns and a larger attack surface than ever. Some of the security challenges that 5G networks will face are as follows.

- The number of IoT devices and other connected things will be significantly high, creating high volumes of traffic.

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 8, Article No. 12 (December 15, 2022)
DOI:*10.22667/ReBiCTE.2022.12.15.012*
*Corresponding author

- Encryption keys for the radio interface may be sent over unreliable/insecure channels.
- Cryptographic integrity protection may be missing in the user data plane.
- Because of service-driven limits on the security architecture, using security measures will be optional.
- When roaming between different operators, user security parameters may not be carried over.
- There could be an increased volume of denial of service (DoS) attacks on the infrastructure.
- Signaling storms could be faced due to distributed control systems requiring coordination.
- In the case of no security measures being taken on the applications, user devices, or operating systems, DoS attacks on end-user devices could have significant effects.

Developments in SDN and NFV and their significant utilization in 5G have brought the complex task of securing a network and its services to another level. An end-to-end approach that takes into account both physical and virtual resources is required for building a robust security ecosystem for SDN and NFV. This end-to-end approach should provide automatic adaptation of security policies to changing conditions in networks. 5G networks, which have SDN and NFV as their basic building blocks, require high reliability in security-related monitoring since network deployments are very dynamic and automated, and SDN/NFV plays an essential role in this automation. In addition to the challenges faced by previous generations of mobile networks, 5G networks will be facing challenges caused by their peculiar characteristics. Security studies for 5G networks, both public and private, have been underway since the beginning of their development and are continuing with efforts from various organizations.

This paper summarizes security issues, existing solutions and standardization efforts for 5G private networks in Europe. The remainder of the paper is organized as follows: Section 2 provides an up-to-date view of 5G private networks and projects in Europe. Section 3 discusses security issues in 5G networks. Section provides an overview of the 5G security architecture. Section 5 discusses 5G security aspects as defined by 3GPP. Section 6 provides a summary of existing approaches that focus on different aspects of 5G networks for securing them. Section 7 provides an overview of the ETSI TS 133 501 standard for 5G network security. Section 8 briefly discusses the EU Toolbox for 5G Security and Section 9 concludes the paper.

2 5G Private Networks in Europe

Unlike the networks that are commonly utilized for their voice and data services, one can define 5G private networks with their proprietary services for private enterprises specialized in transportation, logistics, manufacturing, industrial processing, etc. [3]. The private network infrastructure will be used exclusively by devices with the required authorization and not be publicly accessible by all mobile devices. There are different architecture models for these networks, including completely private networks where all of the network components are operated by a single enterprise, and more hybrid networks where managed services providers or public operators provide access to part of their infrastructure or spectrum. Network slicing will be an important enabler for hybrid public/private networks.

Figures 1, 2, 3, and 4 demonstrate the different deployment scenarios for 5G private networks as discussed by the 5G Alliance for Connected Industries and Automation [4].

European 5G Observatory [3] maintains a list of major 5G private network projects in the European Union. This list includes information on which country the network is deployed in, which companies are

deploying the private network, which sector the network will be utilized for, and what spectrum band is used. One notable example is Germany deciding to allocate a dedicated 100 MHz portion in the 3.7-3.8 GHz range to 5G campus networks.

GSMA Intelligence has recently conducted a survey on the adoption of 5G private networks by enterprises [5]. Based on the survey, 55% of the enterprises consider private wireless networks as significant for successful IoT deployment, but the majority of them do not see security as their responsibility and expect IoT solutions to be secure by default.

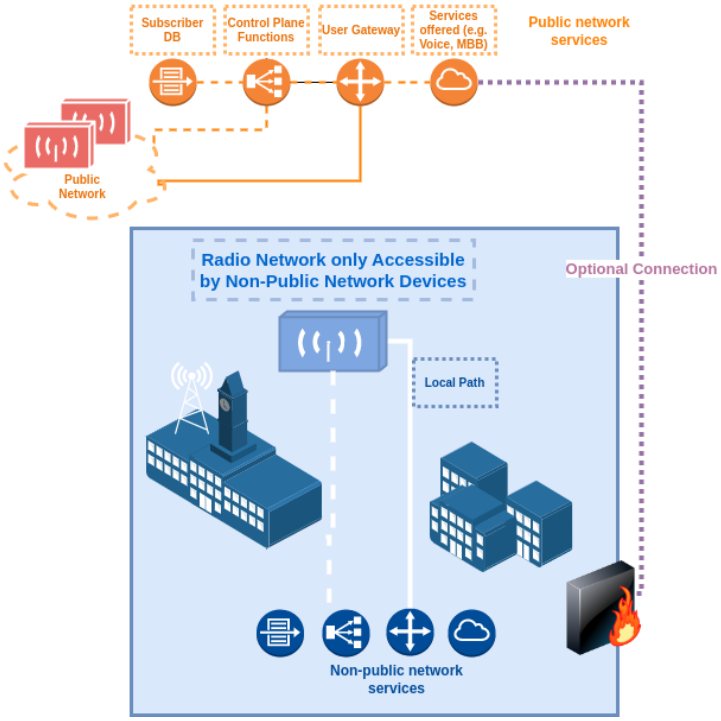

Figure 1: Stand-alone Non-Public Isolated Network

3 Security Issues in 5G Networks

Table 1 provides a summary of the main assets in the 5G infrastructure and the possible threats each could face [6]. The European Union Agency for Cybersecurity (ENISA) published an assessment of the relative importance of the different assets from a security standpoint, considering their roles in achieving confidentiality, integrity, and availability in the network [7]. Core Network Functions (5G Core), Network Functions Virtualization (NFV), and Management and Orchestration (MANO) were identified as the most critical among all 5G assets [6].

The requirements URLCC defines for reliability and availability come with the cost of critical breaches against security with radio jamming and signaling storm attacks. IoT systems due to their heterogeneity have a wide range of security demands, resulting in higher flexibility requirements within the 5G security infrastructure. Below is a list of attacks that could be launched against 5G networks [8].

- `HX-DoS` – This attack integrates HTTP and XML messages to flood scripts and destroy the cloud service provider's ability to communicate through the CPS infrastructure. These attacks are planted

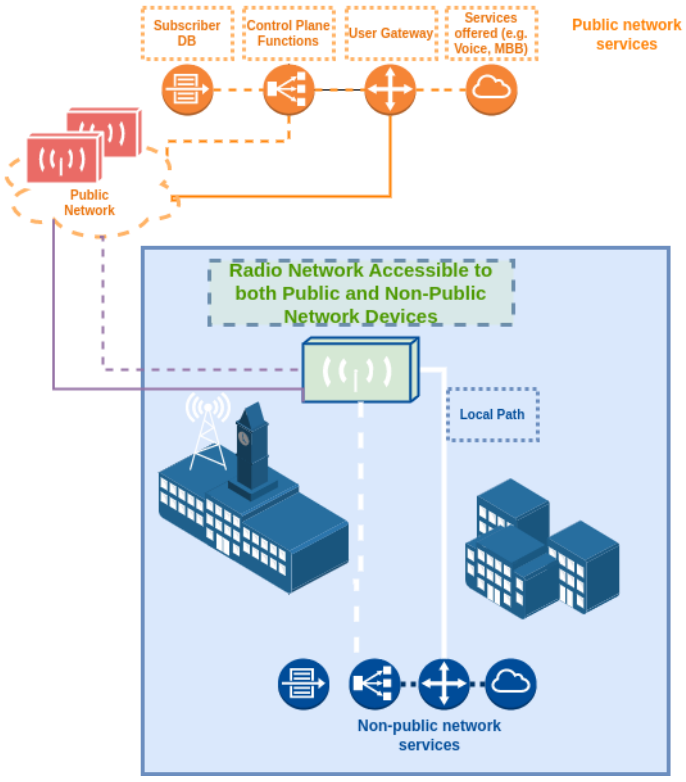

Figure 2: Shared Radio Access Network Deployment

directly within the cloud environment in CPS [9] with the aid of web services like infrastructure as a service (IaaS), platform as a service (PaaS), and service as a service (SaaS). These attacks are quickly resolved, but different issues will arise if they keep happening repeatedly.

- `SIPDAS` – This attack, which is a form of DoS, involves generating a legal SIP INVITE message and transmitting it to the receiver SIP component over the network. It generates a spoofed IP address for TCP or UDP manually, randomly, or by choosing a spoofed IP address from a subnet [10].

- `Byzantine attacks` – This attack involves an adversary modifying selected packets, dropping certain packets, forwarding the majority of the data in its encoded form, and occasionally stopping to send packets it receives, although it remains active in the network.

- `Jamming` – Wireless communication channels used for 5G networks are vulnerable to radio interface attacks. The radio interfaces must operate properly with the use of control channels. High-powered, stealth jamming attacks can be used to block particular control channels used to limit the frequency bands. If a hacker is able to take over several mobile devices and construct a botnet using these compromised targets, the strength of the jammer attacks increases.

- `MitM` – In the man-in-the-middle (MitM) attack, an attacker builds a legitimate communication event between two User Equipments (UEs) over the network, allowing her to seamlessly intercept the communication details and modify the content.

- `DoS` – In a denial of service (DoS) attack against a 5G network, an attempt is made to disable the functions of various types of network resources by consuming their battery, bandwidth, etc.,

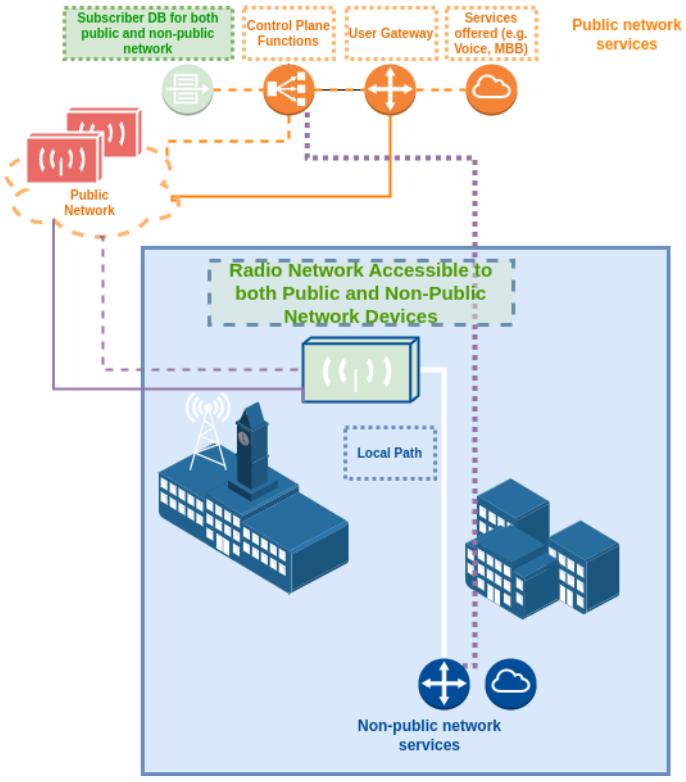

Figure 3: Shared Radio Access Network Deployment with Control Plane

such that they cannot respond to legitimate requests.

- `Spoofing` – On a 5G network, spoofing allows an attacker to intercept legitimate conversations. An attacker injects forged messages using a fake identity to obtain benefits and performs other malicious attacks, including MitM and DoS attacks.
- `Rogue base stations` – In a rogue base stations (RBS) attack, an adversary masquerades as a legitimate base station with the goal of unauthorized access and monitoring within a communication channel. These attacks allow the leakage of private information of mobile subscribers, unwanted advertising, and communication subversion.
- `Eavesdropping` – In the case of an attacker who has access to the transmission channel, s/he can intercept the content over the network without legitimate authorization.
- `Tampering` – In a tampering attack, an attacker can block data transmission or modify the data being transmitted over the network channel without authorization. This will damage efficiency and performance during fog computation. Due to the wireless network and user mobility (UMC), these attacks are hard to spot and can delay or prevent data packet transfers.
- `Smart attacks` – This attack is performed when an attacker can analyze the network status with the use of intelligent radio devices. Based on their distance from the targets, the attacker can launch other attacks, such as spoofing and jamming, using the information gathered from their analysis [11].
- `Privacy leaks` – Both legitimate and illegitimate device owners may leak information from devices, which attackers can take advantage of.

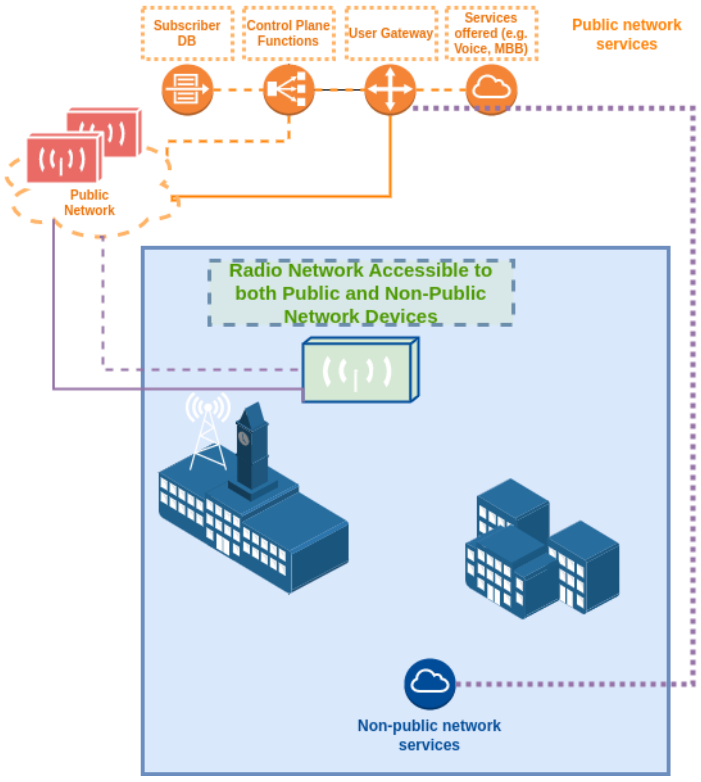

Figure 4: Non-Public Network Deployment in Public Network

- `Hijacking` – An attacker attempts to consume the controller (i.e., data-to-control plane saturation) to disrupt or completely shut down a part of the network.

- `Side-channel attacks` – It is possible to extract sensitive information from physical patterns such as power usage. These types of attacks are called side-channel attacks. 5G networks are significantly more vulnerable to these attacks since they utilize network slicing. This allows an adversary to choose a smaller target space to analyze network parameters.

4 5G Security Architecture

The security backbone of 5G is composed of various protocols, network functions, and components that are responsible for secure and reliable end-to-end communication. There are various specific security mechanisms such as Radio Access Network (RAN) for user access protection, Core Network security (5GC), Edge Computing for perimeter entity security, and NFV security. There is an additional group of security mechanisms for analytics, audit and management activities. Figure 5 below illustrates the 5G security architecture as introduced by 3GPP.

The core network includes home environment (HE) and user equipment (UE) services. HE has a unified data management (UDM) module that works in parallel with the authentication repository and processing function (ARPF). ARPF stores cryptographic algorithm and long-term security parameters. Furthermore, it manages authentication vectors. UE services are the authentication server function (AUSF), the session management function (SMF), and the access mobility management function (AMF). AMF manages signaling, authentication, and authorization operations. It creates keys for different se-

Table 1: 5G Assets and Corresponding Threats [6]

Assets	**Threats**
5G Core	unauthorized access, DDoS, attacks on roaming protocol, NFV-based attacks, data tampering, OSS/5GC attacks
Air interface	SON attack, jamming, eavesdropping, impersonation, data tampering, rough BTS
gNB	Data leakage, hardware/software tampering, RAN DDoS, unauthorized access
MEC	Application layer attacks, untrusted 3rd party applications, DDoS UPF, virtualization attacks, API attacks
O&M	unauthorized access, malware, OSS services integration, data leakage, O&M threats
UE	Malware, cloning, bot hijacking, rough BTS, protocol downgrade, supply chain poisoning, IMSI catching
Transport	Eavesdropping, SDN threats, tampering, protocol downgrade, protocol modification

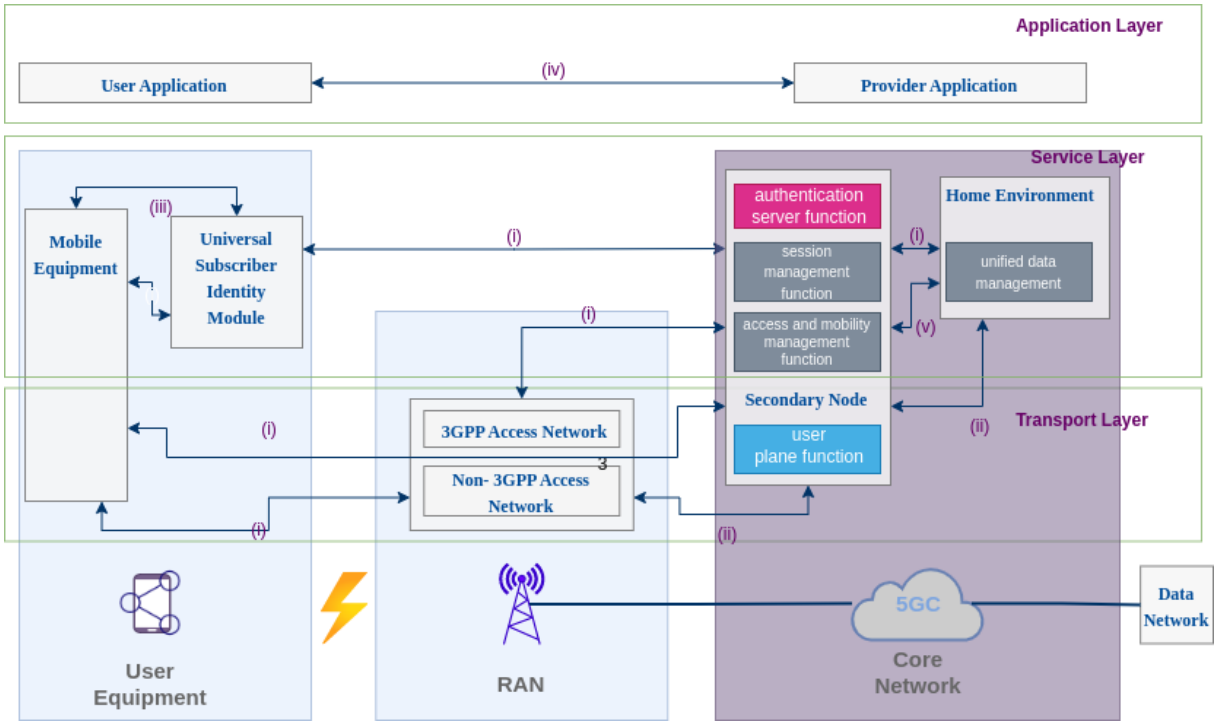

Figure 5: 5G Security Architecture [12].

curity scenarios. SMF handles the secure session management. AUSF interacts with the ARPF module in UDM and handles the termination of requests originating from AMF. AMF module has a security anchor function (SEAF) to manage the primary authentication process by defining the standard anchor

key for all access scenarios. Therefore, AMF in UE provides the basic operations for confidentiality and integrity within a non-access stratum (NAS) within RAN. User plane functions (UPF) are transport-layer functions operating as the secondary nodes for the UE modules. UPF provides traffic flow management and security policies. As described in Figure 5, UE's service and transport layer functions are part of core network operations.

The policy control function (PCF) enables custom security protection. PCF can generate security policies by considering application-level input, network security capability, and UE security capability and provide the policies to other network functions in the control plane (e.g., SMF and AMF). The 3GPP 5G next-generation base stations supporting the new 5G new radio (NR replacing the current LTE base stations) are abbreviated as gNBs in 5G terminology. The PCFs forward the up-to-date policies to the gNB in RANs or UPF modules within its core network. The gNB provides security following operations from AMF for the Access Network stratum (AS) level over the 5G communication interface. UPF is the anchor for mobile users within the 5GC and enables data forwarding operations and security policies. Also, for customized authentication vectors specific to 5G applications, it is possible to produce different network slices [13].

The 5G CHARISMA project([14]) is a security infrastructure developed on top of the ETSI MANO framework that aims to manage and orchestrate the virtual network security operations, parameters, and policies. Figure 6 demonstrates the security management architecture of CHARISMA. This security management architecture (SMA) is divided into two sub-components: Security Policy Management (SPM) and Security & Monitoring Analytics. The SPM provides service-level end-to-end security policies. It translates the existing security policies and compares these policies into specific security requirements. These security requirements are defined in virtual security functions (VSF), supporting the virtual network functions (VNFs) by defining rather concrete security parameters for the virtual machine (VM). SMA manages various resources from the application level (e.g., monitoring data), service level (VNFs), physical layer, and virtual environments and consumes these resources to extract knowledge. The knowledge extracted from these resources can be used for recommendation systems that incorporate intelligent analytics and algorithms on the real-time state information of an entire network. Based on this stateful knowledge and pre-defined service policies, the security policy management can be dynamically observed on a per-tenant basis [15].

With release 15, 3GPP introduced two 5G authentication methods, which include primary and secondary authentication, to accomplish more strict security requirements from certain vertical service providers. Like the 4G system, primary authentication establishes confidence between the user and the network. EAP-AKA (Extensible Authentication Protocol for Authentication and Key Agreement) and 5G-AKA are two methods for the direct authentication technique. The AUSF can select an appropriate authentication vector and its operational specifications according to the user and current network state details. Earlier generations of networks are vulnerable to certain frauds, especially in the home environment. The primary authentication methods are improved to enhance better security control. The AUSF receives the results of the UE authentication procedure during the network visit. The results indicate the success of access. Also, if 3GPP specific parameters are used, the results are sent to the UDM module in the HE. It is possible to monitor the user's actions by analyzing the user authentication status stored within the UDM module [13].

There are two ways to prevent user privacy issues. First, protect the permanent user credentials through encryption. Here, it is crucial to encrypt the mobile subscriber identification number of the IMSI and credentials specific to routing operations. Another way is to conceal this information thoroughly. It is possible to combine these two approaches for greater improvement of privacy. Release 15 by 3GPP proposed two features: the subscription concealed identifier (SUCI) and the subscription identifier de-concealing identifier (SIDF). SUCI is a one-time identifier. The SIDF enables the de-concealing of the SUCI by the secure private key of HE. UE embeds the concealing function in itself. A new SUCI is

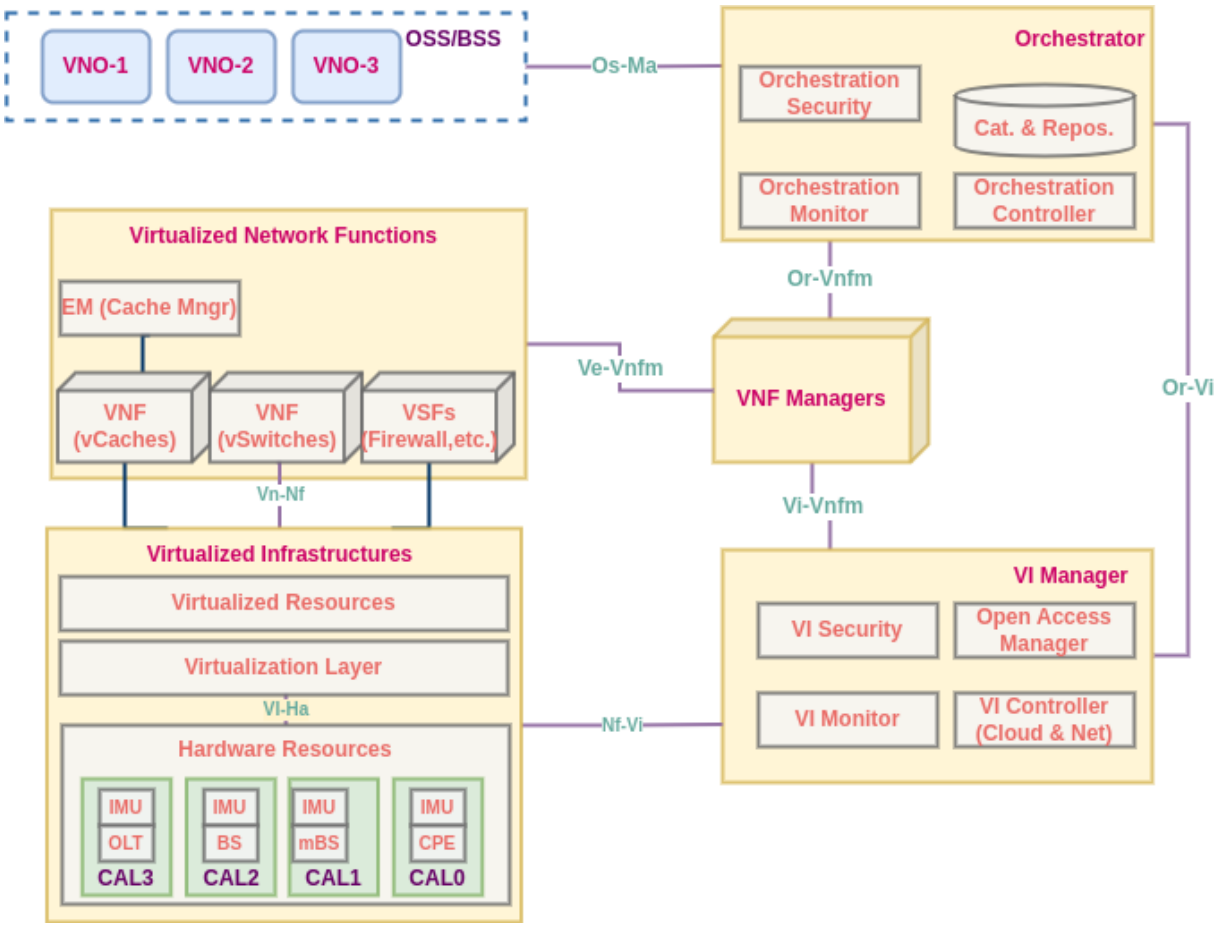

Figure 6: High-Level control, management, and orchestration in 5G CHARISMA Project

generated using the public key that belongs to HE and the elliptic curve cryptography public-private key pair. Therefore, this temporary SUCI is transmitted over an unreliable communication channel instead of the permanent identifier. Therefore, eavesdropping attacks from passive and active adversaries are effectively prevented [13].

5 3GPP 5G Security Aspects

Security of 3GPP 5G networks is challenged by new features and tools such as supporting D2D communication, massive numbers of IoT devices, V2X communication, SDN/NFV, etc. The following five aspects require specific attention when considering 3GPP 5G security.

1. *5G Access and Handover Security* – 5G networks will support large numbers of users and provide secure access to multiple device types. There are many security concerns in the access security aspect of 5G networks, such as ultra-fast multi-domain authentication and authorization, heterogeneous communication, and seamlessly secure handover in roaming between networks.

2. *IoT Security* – In order to account for various IoT technologies, 3GPP has designed many standards, including LTE Enhanced MTC (eMTC) and Narrowband IoT (NB-IoT). eMTC is a technology designed to meet the requirements of existing LTE carrier-based IoT devices. For NB-IoT,

this is the new radio interface technology 3GPP has proposed for IoT. The specification includes the QoS mechanism, network architecture, performance requirements, and discusses security requirements, solutions, etc. However, there are still many security issues to be addressed, including large concurrent secure access to IoT devices, differential privacy for different IoT device types, lightweight security mechanisms, privacy protection, etc.

3. *D2D Security* – Device to Device (D2D) communication is the technology developed to reduce end-to-end latency and meet the design goals of 5G networks. It is a form of direct communication integrated tightly within the 5G core network. It has both centralized and distributed behavior due to its hybrid infrastructure. This heterogeneity makes the system vulnerable to threats arising from cellular and ad-hoc networks.

4. *V2X Security* – 5G-V2X is built on top of Dedicated Short Range Communications in vehicular mechanisms. In terms of communications, it involves broader coverage, additional QoS features, scalability, and tightened security. However, these improvements have not affected the security and performance costs that come with a centralized structure, a wide range of authentication scenarios, internal privacy issues within V2X user equipment, and broadcast message security in multiple V2X UE device communications.

5. *Network Slicing Security* – As 5G networks will have SDN and NFV as their underlying technologies, the core network topology will be flatter, and the network resources and relay node resources will be controllable and optimized for flexibility. However, due to different network characteristics resulting from the utilization of SDN/NFV, previously utilized methods for security, security policies, trust management policies, etc., which were originally designed for traditional networks may not be applicable in 5G [16].

3GPP has listed several important 5G security mechanisms. Firstly, UE access control enables protection against rogue base stations through a bidirectional authentication mechanism. Secondly, using 256-bit key encryption algorithms, SUCIs for HE identification, and mobile subscriber identity numbers (MSIN) in their encrypted form provide confidentiality and integrity. Lastly, information security can be achieved through the use of IPsec between 3GPP Network Elements (NEs), such as security edge protection proxy (SEPP) situated between the Home Public Land Mobile Network (HPLMN) and Visited Public Land Mobile Network (VPLMN), and HTTPS used between 5G core network service functions [6]. The HPLMN identifier is derived from IMSIN, whereas the VPLMN identifier is derived from the live network while the subscriber is attached to the network.

Inter-domain interfaces and intra-domain interfaces and equipment are protected using security gateways (SeGW). Examples include IPSec tunnels and firewalls for access control. The security of services is ensured by the application layer.

6 Existing 5G Security Approaches

Achieving end-to-end security in 5G networks involves securing many components of the infrastructure and has been a widely studied topic since the start of 5G discussions. Below we provide a summary of existing works in 5G security, categorized by their security targets.

Security in 5G Access. Authentication and key agreement are among the most important security issues in 5G access, and have been the focus of both research and industry since the introduction of 5G networks. A USIM-compatible 5G-AKA protocol was proposed in [17]. In this scheme, the 5G-AKA

protocol cooperates with the Diffie Hellman Key Exchange (DHKE) cryptographic protocol. Therefore, the session key generation is based on the long-term secret information and Temporary DH parameters. The scheme can ensure Perfect Forward Secrecy (PFS) and resist passive cryptanalysis attacks. However, the DH algorithm imposes computational and communication costs for resource-constrained mobile devices. A new scheme proposed by Liu et al. [18] also achieves PFS with additional credential disclosure of encrypted credential information. Furthermore, it is resistant against replay attacks with the use of a nonce value and an additional passcode. This scheme also incorporates a tuple of authentication error information (MAC_FAIL, SYNC_FAIL) that is sent to SEAF using the same format as [17] and performs DHKE encryption. Therefore, it can avoid traceability attacks [19].

Authentication and data transmission for V2X systems. Fast and reliable authentication is a major issue in V2X systems. Ometov and Bezzateev showed an improvement in availability by introducing Multi-Factor Authentication (MFA) in existing media systems [20], as an extension to Single-Factor Authentication (SFA). An MFA system is based on the Lagrange polynomial of Shamir's Secret Sharing scheme to provide a flexible authentication mechanism for V2X applications. The system can evaluate the missing factor for user authentication without providing sensitive biometric data to the verification entity [19]. The authors state that the CLASC scheme can be implemented on control centers, vehicles, smart devices, roadside units, and cloud servers. In [21], a secure and efficient identity-based message authentication scheme is proposed for LTE-V networks. This scheme has additional privacy properties through pseudo-identification. It also has the non-repudiation property of single and bulk messages to reduce the signaling exchanges. The authors in [22] designed an anonymous handover authentication protocol for LTE-A vehicle networks with the use of elliptic curve cryptography (ECC). They showed that ECC provides more efficient and secure improvements compared to Diffie-Hellman and Discrete Logarithm based authentication.

5G new radio security. The 3GPP on the physical layer in terms of security has been addressed by many academic works despite its slow progress [23, 24, 25]. Physical layer security (PHY-SEC) requires more attention due to its observable intrinsic random capabilities within its radio communication medium [23]. The computational complexities and following costs originating from upper-layer security protocols do not affect the physical layer [23]. PHY-SEC is capable of securing the communication whereas upper-layer encryption mechanisms can protect the processed data. These two approaches used together can result in the efficient and private transmission of secret information within 5G networks. The term confidentiality here refers to the maximum secure throughput during the communication to authenticated parties that takes place in an unreliable channel with possible eavesdroppers. With reasonable encryption and computational costs, such communication is possible. Additionally, taking advantage of the physical uniform characteristics of channel state information (CSI) we can generate secure and unique keys for each edge device within a network [26, 27, 28], using the received signal strength (RSS) [29, 30] or direct information [31]. We can generate and disseminate secure keys that are extensible for physical layer authentication [32, 33, 34]. PHY-SEC has evolved with the introduction of non-attenuated channels, relay channels [35], and multi-antenna channels [36]. With the advent of new 5G radio technologies such as mmWave, 3D MIMO [37], M-MIMO, Full Duplex, and Cooperative Forwarding, theoretical and practical secrecy capabilities in new channels have become an area of increasing interest [3].

Secure SDN-based network. Since the introduction of 5G networks, many research efforts have been dedicated to SDN security threats [38, 39, 40]. Various network programming languages such as Frentic [41] and Procera [42] have been proposed for SDN security. Granular access control and authorization mechanisms provide a security layer to the control plane of SDN [43]. There are also dynamic

access control systems designed to protect the control plane [44]. Solutions for availability at the control layer include minimizing controller load, distributing features, processing performance methods, and reliable placement [45, 46, 47]. There are also security mechanisms for the SDN data plane. Some of these include granular security enforcement methods specific to authentication. There are also others offering authorization mechanisms. These mechanisms provide policies for installation and modification [48]. FlowChecker [49] was proposed to detect anomalies within forwarding tables on many data path switches. The work in [50] designed a debugging tool for these anomaly states within the tables to detect illegitimate activities within the network. There are forms of SDNs for centralized control over network activities and with transparent states and dynamic forwarding rule updates. These improve the performance of other network security mechanisms [51]. In [52], a dynamic network-wide security infrastructure with rapid reaction mechanisms to prevent incoming possible threats. The control plane structure of SDN allows definitive traffic pattern analysis from legitimate monitoring network nodes to identify network inconsistencies. Dynamic traffic flow control allows rapid anomaly detection and integration of an intrusion detection system or a firewall to perform at runtime.

Many network functions can be structured into an SDN with application programming interfaces (APIs). However, this can expose critical features of a network against malicious applications. This can result in wide-ranged disruption of the network [1]. OpenFlow is a widely used SDN architecture that allows the storage of traffic flow data through forwarding system elements until the control plane terminates the modification of forwarding rules. This will allow reviewing the incoming modification requests from suspicious sources. In addition, this controller dependency requires channeling of control data planes that are resistant to cyber attacks. With total network visibility, centralized control, and programmability across network elements, SDN makes it possible to enforce security policies across the entire network and provides rapid discovery of threats through gathering information from network resources, states, and flows. Since most of the security functionality is implemented in the software application plane, SDN leverages security which can be referred to as software-defined security.

AI-based approaches. Artificial Intelligence (AI) is one of the major research areas for 5G security for identification and prevention mechanisms against malicious systems. There are many methods categorized under machine learning and deep learning systems that allow efficient and reliable, automated predictive decision-making. 5G technology requirements can be realized with the aid of AI-driven methods for the network system to meet exceptional Quality of Experience (QoE) requirements. Integrated mechanisms can predict network performance degradation by actively analyzing live traffic at an SDN-enabled switch. The threats explained in the previous sections can be structured into vectors to use as historical flow patterns for future traffic analysis. Recent solutions use Reinforcement Learning (RL) and Deep Reinforcement Learning (DRL) techniques to deal with such attacks. DRL methods provide autonomous capabilities to the systems from time-varying observations to generate optimal actions. These actions can result in robust and dynamic security operations. DRLs also provide good collaborative methods. Deep learning (DL) methods can extract information from more complex patterns from past inputs with its multi-layered data filtering architecture. Other than recent methods such as artificial neural networks and deep learning techniques, we can also make use of traditional machine learning based classification algorithms. These predictions can be performed in a real-time manner as well.

AI and ML can work efficiently within a highly data-driven environment and can collaborate with virtualized network elements. They enable dynamic and powerful solutions for security and privacy for 5G systems. AI and ML can improve the infrastructure in terms of computational and production costs.

We can build applications such as virus scanning systems, complex intrusion detection systems, spam filters, and fraud detection systems using AI and ML methods. These methods require data from the live network traffic, stored procedures, and many more. DL has been implemented in service-level security

(e.g., anomaly detection), application-level system integrity (e.g., malware, virus, and botnets observed in mobile networks), and application-level user privacy (e.g., protection of personal information including activity logs) [13]. DL has provided many solutions to such security issues with methods such as feedforward autoencoder, dense and convolutional neural networks, and recurrent neural networks. At the service-level security, they have been used against malware, DoS, flood, side-channel, and many other attacks. At application-level security, from a system integrity point of view, DL mechanisms have been able to classify malicious requests from applications, spam messages, unknown incoming traffic, and botnets. From a user privacy point of view, they have been used to detect illegitimate data sharing, information leakage, and unauthorized access to another user's private information. However, the processing of data during the ML operation has its risks. They can be used for malicious purposes. Even when the processed data is discarded and no longer available, the residue of operations can be analyzed with data mining operations.

Table 2 provides a summary of security challenges specific to 5G and the corresponding solution approaches.

Table 2: 5G Security Challenges and Corresponding Solutions [13]

Challenge	**Countermeasure**
Limitations of 4G architecture	5G security architecture, new key hierarchy
IoT requirements: low-power processing, remote credential provisioning, device authentication	Lightweight cryptographic algorithms, network slicing, scalable key management
Risks from new business model: malicious applications, attacks targeting exposure interface	Authentication against applications, TLS-based exposure interface
Need for new trust model	EAP-based secondary authentication
Attacks on NFVO, VNFs, NFVI	Slice access control, protection mechanisms for NFVO, VNF and NFVI
Attacks targeting SDN	Secure application development, control plane protection, data plane protection
Service-based architecture risks: spoofing between network functions, MitM attacks between network functions	TLS-based authentication between network functions, network function authentication during registration
Mobile edge computing risks	5G security architecture, secure network exposure
Device-to-device (D2D) communication risks: impersonation, eavesdropping	Secure D2D with key management, authentication, confidentiality/integrity protection mechanisms
Risks from new radio technologies	5G new radio security: Physical layer authentication, channel adaption, encryption by channel coding, artificial noise

7 ETSI TS 133 501

The European Telecommunications Standards Institute released Technical Specification 133 501, which specifies the security architecture, and the security procedures performed within the 5G System including the 5G Core and the 5G New Radio [53]. This document provides comprehensive guidelines on the

security requirements on UE, gNB, ng-eNB, AMF, SEAF, ADM, AUSF and core network security and presents security procedures between UE and 5G network functions.

Annex B of the document provides an example of using additional EAP methods for primary authentication in private networks, which uses the 5G system specified in TS 22.261. It aims to demonstrate the application of the 5G authentication framework for primary authentication to EAP methods different from EAP-AKA. These other EAP methods are only intended for use in private networks or when IoT devices in isolated deployment scenarios are involved, i.e. they do not consider roaming. In 5G private networks, the SUPI and SUCI should be encoded using the NAI format as specified in TS 23.501. User equipments always include the realm part in the NAI so that packets can be routed to the correct UDM.

8 EU Toolbox for 5G Security

The European Commission adopted its recommendation on the cyber security of 5G networks on 26 March 2019, after the support of the European Council expressed on 22 March 2019 for a collective approach to 5G network security. A recommendation is required for the EU-wide risk assessments and reviews of the national measures on the cyber security of 5G networks for an agreement on standard risk analysis and the development of a toolbox to prevent security threats [54]. The deployment of a toolkit can create a common ground for security risks within 5G networks and provide a roadmap to prevent these risks at the EU level as shown in Table 3. Wrongly configured networks or insufficient access controls result from inadequate security measures. 5G supply chain-based risks are low product quality, dependency on a single supplier, or homogeneity of supplier types. Active attackers can cause state interference within the 5G supply chain and criminal exploitation of a 5G network by hostile persons. The issues in the existence of interdependencies between 5G and critical infrastructures can disrupt vital services (e.g., healthcare systems). The information flow can be disrupted by electricity supply or other interconnected infrastructures when there is a tight dependency between the 5G network and the critical system. End-user devices such as smartphones, IoT appliances, tablets, wearable devices, and personal computers are prone to exploitation.

The EU coordinated risk assessment identifies several types of risks of strategic importance from the EU point of view illustrated by specific risk scenarios, as shown below. They reflect the relevant combination of vulnerabilities, threats, and threat actors and assets identified.

Strategic measures include measures related to strengthening the regulatory powers of competent authorities for controlling network acquisition and deployment, as well as specific criteria for dealing with risks associated with non-technical vulnerabilities, such as the risk of interference by a third country or risk of dependency. They also include initiatives to advance sustainable 5G supply and make value chains sustainable and diversified to avoid the risk of systemic dependence in the long term. Strategic measures have the potential to be highly effective in addressing certain 5G cyber security risks identified in the EU joint risk assessment report, including the following strategic criteria:

- `SM01` – Stronger regulatory powers for appropriate institutions.
- `SM02` – Inspecting authorized operators and collecting information from them.
- `SM03` – Building risk profiles on supplier entities and implementing certain policies on different risk groups
- `SM04` – Monitoring of service providers and third-party supplier support.
- `SM05` – Deployment of multi-vendor strategies supporting the diversity among suppliers belonging to different mobile network operators.

Table 3: Summary of Risks in EU Coordinated Risk Assessment Report

Risk scenario category	**Risk**
Insufficient security	R1 - Misconfigured networks R2 - Insufficient access control
5G supply chain	R3 - Low quality products R4 - Depending on a single supplier and/or lack of diversity
Operation mode of main threat actors	R5 - Interference of state actors through 5G supply chain R6 - Network exploitation by organized crime or crime groups
5G network-critical system interdependencies	R7 - Disruptions in services or critical infrastructure R8 - Massive network failure caused by electricity supply or support system interruption
End user devices	R9 - Attacks targeting smart devices, IoT or handsets

- SM06 – Higher resilience in a wider range.
- SM07&SM08 – Progressive improvement toward scalable and sustainable network ecosystem within Europe Union.

Technical measures . These are intended to support 5G network security by considering the security of physical factors, technologies, people, and processes. The efficiency of these measurements relies on the number of risks observed and the range of the observation measures. Particularly, all technical measures only apply to technical vulnerabilities. Non-technical vulnerabilities are not addressed within this scope (e.g., interferences of a third country). Technical measures include the following:

- TM01 – The aim of a secure design network and architecture is critical baseline security.
- TM02 – The evaluation and assurance of compliance with 5G standards for proposed security measures.
- TM03 – Providing rigid access control policies and mechanisms.
- TM04 – Strengthening of VNF security.
- TM05 – Secure network management, process, and maintenance over 5GC.
- TM06 – Improving of physical security.
- TM07 – Strengthening software update and patch management in terms of security.
- TM08 – Enhancing the supplier security mechanisms and dynamic monitoring of their potential risks.
- TM09 – Requiring EU-issued certification for 5GC equipment and supplier services.

- TM10 – Requiring EU-issued certification for non-5GC ICT products and services such as (e.g., cloud services).

Stakeholders will play an important role in the 5G ecosystem. These entities will ensure network security at different levels. The following is a list of the stakeholders in 5G security:

- Internet Exchange Points
- National Regulators
- Centers for information analysis and sharing
- National centers, coordinators and agencies for cyber security
- Test Centers for 5G
- Certification Authorities
- Government institutions and services

The entities above may have varying degrees of interest in 5G assets, including being responsible for mitigating the risks to these assets. They need to develop independent or co-responsible strategies to reduce exposure to cyber threats.

The EU Agency for Cybersecurity (ENISA). ENISA is one of the important organizations supporting EU member states for secure deployment of 5G networks. One prominent instance where ENISA offered strong support for the European Commission and the EU Member States in 5G network security has been the development of the EU toolbox for 5G security. They have released a number of documents proposing good practices for 5G security, available through their website [55].

9 Conclusion

5G and beyond networks will support many use cases not encountered in the previous generations of mobile networks. The opportunity to form private networks utilizing 5G infrastructure is an important feature, which has already found use in scenarios such as industrial IoT. In this paper we provided a survey of security challenges faced by 5G private networks in Europe and solutions proposed on the various security aspects by researchers and relevant organizations. Despite research and development efforts in 5G private network security that have been going on since the introduction of 5G networks, there is still a clear need for development of security standards in many aspects of 5G networks for achieving strong security without compromising performance.

Acknowledgement

The authors would like to thank Ali Kömürcü for his help with the literature review.

References

[1] European Commission. 5g ppp phase1 security landscape. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf" [Online; Accessed on December 3, 2022].

[2] A. Ijaz, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov. Overview of 5g security challenges and solutions. *IEEE Communications Standards Magazine*, 2(1):36–43, March 2018.

[3] F. Pujol. Private networks – 5g observatory. European 5G Observatory. https://5gobservatory.eu/5g-private-networks/ [Online; Accessed on December 3, 2022].

[4] 5g non-public networks for industrial scenarios. 5G Alliance for Connected Industries and Automation, 2021. https://5g-acia.org/wp-content/uploads/5G-ACIA_5G_Non-Public_Networks_for_Industrial_Scenarios_09-2021.pdf [Online; Accessed on December 3, 2022].

[5] Securing private networks in the 5g era. GSMA Intelligence, 2021. https://assets.foleon.com/eu-west-2/uploads-7e3kk3/4816/securing_private_networks_in_the_5g_era.461381fec79c.pdf [Online; Accessed on December 3, 2022].

[6] D. Soldani. 5g and the future of security in ict. In *Proc. of the 29th International Telecommunication Networks and Applications Conference (ITNAC'19), Auckland, New Zealand*, pages 1–8. IEEE, April 2019.

[7] Marco Lourenco and Louis Marinos. Enisa threat landscape for 5g networks. Technical report, 11 2019.

[8] Jin Ho Park, Shailendra Rathore, Sushil Kumar Singh, Mikail Mohammed Salim, AE Azzaoui, Tae Woo Kim, Yi Pan, and Jong Hyuk Park. A comprehensive survey on core technologies and services for 5g security: taxonomies, issues, and solutions. *Human-centric Computing and Information Sciences*, 11(3):1–22, January 2021.

[9] Ashley Chonka and Jemal Abawajy. Detecting and mitigating hx-dos attacks against cloud web services. In *Proc. of the 15th International Conference on Network-Based Information Systems, Melbourne, VIC, Australia*, pages 429–434. IEEE, November 2012.

[10] Melih Tas. Sip-das., 2020. https://github.com/cys3c/SIP-DAS [Online; Accessed on December 3, 2022].

[11] Liang Xiao, Caixia Xie, Tianhua Chen, Huaiyu Dai, and H. Vincent Poor. Mobile offloading game against smart attacks. In *Proc. of the 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'16), San Francisco, CA, USA*, pages 403–408. IEEE, September 2016.

[12] Xiaowei Zhang, Andreas Kunz, and Stefan Schröder. Overview of 5g security in 3gpp. In *Proc. of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN'17), Helsinki, Finland*, pages 181–186. IEEE, October 2017.

[13] Shunliang Zhang, Yongming Wang, and Weihua Zhou. Towards secure 5g networks: A survey. *Computer Networks*, 162:106871, October 2019.

[14] M.C. Parker, G. Koczian, F. Adeyemi-Ejeye, T. Quinlan, S.D. Walker, A. Legarrea, M.S. Siddiqui, E. Escalona, S. Spirou, D. Kritharidis, K. Habel, V. Jungnickel, E. Trouva, A. Kourtis, Y. Liu, M. Sander Frigau, J.C. Point, G. Lyberopoulos, E. Theodoropoulou, K. Filis, Th. Rokkas, I. Neokosmidis, D. Levi, E. Zetserov, A. Foglar, M. Ulbricht, B. Peternel, and D. Gustincic. Charisma: Converged heterogeneous advanced 5g cloud-ran architecture for intelligent and secure media access. In *Proc. of the 3rd European Conference on Networks and Communications (EuCNC'16), Athens, Greece*, pages 240–244. IEEE, September 2016.

[15] Pouria Sayyad Khodashenas, J Aznar, A Legarrea, C Ruiz, Muhammad Shuaib Siddiqui, Eduard Escalona, and Sergi Figuerola. 5g network challenges and realization insights. In *Proc. of the 18th International Conference on Transparent Optical Networks (ICTON'16), Trento, Italy*, pages 1–4. IEEE, August 2016.

[16] Jin Cao, Maode Ma, Hui Li, Ruhui Ma, Yunqing Sun, Pu Yu, and Lihui Xiong. A survey on security aspects for 3gpp 5g networks. *IEEE Communications Surveys & Tutorials*, 22(1):170–195, November 2019.

[17] Jari Arkko, Karl Norrman, Mats Näslund, and Bengt Sahlin. A usim compatible 5g aka protocol with perfect forward secrecy. In *Proc. of the 2015 IEEE TrustCom/BigDataSE/ISPA, Helsinki, Finland*, pages 1205–1209. IEEE, August 2015.

[18] Fuwen Liu, Jin Peng, and Min Zuo. Toward a secure access to 5g network. In *Proc. of the 2018 IEEE*

TrustCom/BigDataSE, New York, NY, USA, pages 1121–1128. IEEE, September 2018.

[19] Sonakshi Vij and Amita Jain. 5g: Evolution of a secure mobile technology. In *Proc. of the 3rd International Conference on Computing for Sustainable Global Development (INDIACom'16), New Delhi, India*, pages 2192–2196. IEEE, October 2016.

[20] Aleksandr Ometov and Sergey Bezzateev. Multi-factor authentication: A survey and challenges in v2x applications. In *Proc. of the 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT'17), Munich, Germany*, pages 129–136. IEEE, January 2017.

[21] Cheng Xu, Xiaohong Huang, Maode Ma, and Hong Bao. A secure and efficient message authentication scheme for vehicular networks based on lte-v. *KSII Transactions on Internet and Information Systems (TIIS)*, 12(6):2841–2860, January 2018.

[22] Cheng Xu, Xiaohong Huang, Maode Ma, and Hong Bao. An anonymous handover authentication scheme based on lte-a for vehicular networks. *Wireless Communications and Mobile Computing*, 2018:1–15, July 2018.

[23] Nan Yang, Lifeng Wang, Giovanni Geraci, Maged Elkashlan, Jinhong Yuan, and Marco Di Renzo. Safeguarding 5g wireless communication networks using physical layer security. *IEEE Communications Magazine*, 53(4):20–27, April 2015.

[24] Sreeram Munisankaraiah and A Arun Kumar. Physical layer security in 5g wireless networks for data protection. In *Proc. of the 2nd International Conference on Next Generation Computing Technologies (NGCT'16), Dehradun, India*, pages 883–887. IEEE, March 2016.

[25] Yongpeng Wu, Ashish Khisti, Chengshan Xiao, Giuseppe Caire, Kai-Kit Wong, and Xiqi Gao. A survey of physical layer security techniques for 5g wireless networks and challenges ahead. *IEEE Journal on Selected Areas in Communications*, 36(4):679–695, April 2018.

[26] Sanghun Im, Jinho Choi, and Jeongseok Ha. Secret key agreement for massive mimo systems with two-way training under pilot contamination attack. In *Proc. of the 2015 IEEE Globecom Workshops (GC Wkshps'15), San Diego, CA, USA*, pages 1–6. IEEE, February 2015.

[27] Kai Zeng. Physical layer key generation in wireless networks: challenges and opportunities. *IEEE Communications Magazine*, 53(6):33–39, June 2015.

[28] Chan Dai Truyen Thai, Jemin Lee, and Tony QS Quek. Physical-layer secret key generation with colluding untrusted relays. *IEEE Transactions on Wireless Communications*, 15(2):1517–1530, October 2015.

[29] Kui Ren, Hai Su, and Qian Wang. Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wireless Communications*, 18(4):6–12, August 2011.

[30] Yu Luo, Lina Pu, Zheng Peng, and Zhijie Shi. Rss-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements. *IEEE Communications Magazine*, 54(2):32–38, February 2016.

[31] Hasan Taha and Emad Alsusa. Physical layer secret key exchange using phase randomization in mimo-ofdm. In *Proc. of the 2015 IEEE Global Communications Conference (GLOBECOM'15), San Diego, CA, USA*, pages 1–6. IEEE, December 2015.

[32] Nate Goergen, W Sabrina Lin, KJ Ray Liu, and T Charles Clancy. Extrinsic channel-like fingerprint embedding for authenticating mimo systems. *IEEE Transactions on Wireless Communications*, 10(12):4270–4281, December 2011.

[33] Dan Shan, Kai Zeng, Weidong Xiang, Paul Richardson, and Yan Dong. Phy-cram: Physical layer challenge-response authentication mechanism for wireless networks. *IEEE Journal on Selected Areas in Communications*, 31(9):1817–1827, August 2013.

[34] Xiaofu Wu and Zhen Yang. Physical-layer authentication for multi-carrier transmission. *IEEE Communications Letters*, 19(1):74–77, November 2014.

[35] Ye Yang, Qiang Li, Wing-Kin Ma, Jianhua Ge, and PC Ching. Cooperative secure beamforming for af relay networks with multiple eavesdroppers. *IEEE Signal Processing Letters*, 20(1):35–38, November 2012.

[36] Qiang Li, Mingyi Hong, Hoi-To Wai, Ya-Feng Liu, Wing-Kin Ma, and Zhi-Quan Luo. Transmit solutions for mimo wiretap channels using alternating optimization. *IEEE Journal on Selected Areas in Communications*, 31(9):1714–1727, August 2013.

[37] Weidong Zhang, Ying Wang, Fei Peng, and Yuan Yuan. Interference coordination with vertical beamforming

in 3d mimo-ofdma networks. *IEEE Communications Letters*, 18(1):34–37, November 2014.

[38] Sandra Scott-Hayward, Sriram Natarajan, and Sakir Sezer. A survey of security in software defined networks. *IEEE Communications Surveys & Tutorials*, 18(1):623–654, July 2016.

[39] Ijaz Ahmad, Suneth Namal, Mika Ylianttila, and Andrei Gurtov. Security in software defined networks: A survey. *IEEE Communications Surveys & Tutorials*, 17(4):2317–2346, August 2015.

[40] Danda B. Rawat and Swetha R. Reddy. Software defined networking architecture, security and energy efficiency: A survey. *IEEE Communications Surveys & Tutorials*, 19(1):325–346, October 2017.

[41] Nate Foster, Rob Harrison, Michael J. Freedman, Christopher Monsanto, Jennifer Rexford, Alec Story, and David Walker. Frenetic: A network programming language. *SIGPLAN Not.*, 46(9):279–291, September 2011.

[42] Andreas Voellmy, Hyojoon Kim, and Nick Feamster. Procera: A language for high-level reactive network control. In *Proc. of the 1st Workshop on Hot Topics in Software Defined Networks, Helsinki, Finland*, page 43–48. ACM, August 2012.

[43] Xitao Wen, Yan Chen, Chengchen Hu, Chao Shi, and Yi Wang. Towards a secure controller platform for openflow applications. In *Proc. of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, Hong Kong, China*, page 171–172. ACM, August 2013.

[44] Yuchia Tseng, Montida Pattaranantakul, Ruan He, Zonghua Zhang, and Farid Naït-Abdesselam. Controller dac: Securing sdn controller with dynamic access control. In *Proc. of the 2017 IEEE International Conference on Communications (ICC'15), Paris, France*, pages 1–6. IEEE, July 2017.

[45] Phillip Porras, S. Cheung, Martin Fong, Keith Skinner, and Vinod Yegneswaran. Securing the software defined network control layer. In *Proc. of the 22nd Network and Distributed System Security Symposium, San Diego, California, USA*, pages 1–15. The Internet Society, January 2015.

[46] Kévin Phemius, Mathieu Bouet, and Jérémie Leguay. Disco: Distributed multi-domain sdn controllers. In *Proc. of the 2014 IEEE Network Operations and Management Symposium (NOMS'14), Krakow, Poland*, pages 1–4. IEEE, May 2014.

[47] Yannan Hu, Wang Wendong, Xiangyang Gong, Xirong Que, and Cheng Shiduan. Reliability-aware controller placement for software-defined networks. In *Proc. of the 13th IFIP/IEEE International Symposium on Integrated Network Management (IM'13), Ghent, Belgium*, pages 672–675. IEEE, May 2013.

[48] Philip Porras, Seungwon Shin, Vinod Yegneswaran, Martin Fong, Mabry Tyson, and Guofei Gu. A security enforcement kernel for openflow networks. In *Proc. of the 1st Workshop on Hot Topics in Software Defined Networks, Helsinki, Finland*, pages 121—-126. ACM, August 2012.

[49] Ehab Al-Shaer and Saeed Al-Haj. Flowchecker: Configuration analysis and verification of federated openflow infrastructures. In *Proc. of the 3rd ACM Workshop on Assurable and Usable Security Configuration, Chicago, Illinois, USA*, page 37–44. ACM, October 2010.

[50] Ahmed Khurshid, Wenxuan Zhou, Matthew Caesar, and P. Brighten Godfrey. Veriflow: Verifying network-wide invariants in real time. *ACM SIGCOMM Computer Communication Review*, 42(4):467–472, October 2012.

[51] Seungwon Shin, Lei Xu, Sungmin Hong, and Guofei Gu. Enhancing network security through software defined networking (sdn). In *Proc. of the 25th International Conference on Computer Communication and Networks (ICCCN'16), Waikoloa, HI, USA*, pages 1–9. IEEE, September 2016.

[52] Jerome Francois and Olivier Festor. Anomaly traceback using software defined networking. In *Proc. of the 2014 IEEE International Workshop on Information Forensics and Security (WIFS'14), Atlanta, GA, USA*, pages 203–208. IEEE, December 2014.

[53] Security architecture and procedures for 5g system. `https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf` [Online; Accessed on December 3, 2022].

[54] Cybersecurity of 5g networks - eu toolbox of risk mitigating measures — shaping europe's digital future. European Commission,, 2020. `https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures` [Online; Accessed on December 3, 2022].

[55] Tackling security challenges in 5g networks. `https://www.enisa.europa.eu/news/enisa-news/`

tackling-security-challenges-in-5g-networks [Online; Accessed on December 3, 2022].

Author Biography

Pelin Angin is an Assistant Professor of Computer Engineering at Middle East Technical University. She completed her B.S. in Computer Engineering at Bilkent University in 2007 and her Ph.D. in Computer Science at Purdue University, USA in 2013. Between 2014-2016, she worked as a Visiting Assistant Professor and Postdoctoral Researcher at Purdue University. Her research interests lie in the fields of cloud computing and IoT security, distributed systems, 5G networks and blockchain. She is among the founding members of the Systems Security Research Laboratory and an affiliate of the Wireless Systems, Networks and Cybersecurity Laboratory at METU. She serves on the editorial boards of multiple journals on IoT, wireless networks and mobile computing.

Manolya Atalay is a PhD Candidate and Research Assistant at Middle East Technical University. Her research interests include Internet of Things, Computer Networks, Cyber Security, Cryptography, Artificial Intelligence, and Software Engineering. She did her Master of Science in Akdeniz University on access control and authentication systems for Internet of Things. Prior to that she worked in smart home applications in AYPRO, power line systems in B-Mühendislik, petroleum and gas loading systems and SAP integrations in Mega Endustries for Tupras, Shell HQ, and Türkiye Petrolleri, Mobile softwares in RnR Associates (Florida, USA), and RF card systems in Oytek Teknoloji and PDI-Erkom. She did her Bachelor of Science at Dokuz Eylül University.

Fatma Ceyda Gokce is a B.S. student in the Department of Computer Engineering at Middle East Technical University. Her research interests lie mainly in the fields of artificial intelligence, machine learning and 5G networks.

Ilsun You received the MS and PhD degrees in computer science from Dankook University, Seoul, Korea, in 1997 and 2002, respectively. He received the second PhD degree from Kyushu University, Japan, in 2012. Now, he is a full professor at Department of Information Security, Cryptology, and Mathematics, Kookmin University. He has served or is currently serving as a Steering Chair, General Chair or a Program Chair of international conferences and symposiums such as MobiSec'16-21, WISA'19-20, ProvSec'18, ACM MIST'15-17 and so forth. Dr. YOU is an associate EiC of Intelligent Automation & Soft Computing (IASC) while being in the Editorial Board for Information Sciences, International Journal of Intelligent Systems, IEEE Access, International Journal of Ad Hoc and Ubiquitous Computing, and ICT Express. Especially, he has focused on 5/6G security, security for wireless networks & mobile internet, IoT/CPS security and so forth while publishing more than 180 papers in these areas. He is a Fellow of the IET and a Senior member of the IEEE.