A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions

Rabia Khan, *Student Member, IEEE,* Pardeep Kumar *Member, IEEE,* Dushantha Nalin K. Jayakody*, *Senior Member, IEEE* and Madhusanka Liyanage, *Member, IEEE*

***Abstract*—Security has become the primary concern in many telecommunications industries today as risks can have high consequences. Especially, as the core and enable technologies will be associated with 5G network, the confidential information will move at all layers in future wireless systems. Several incidents revealed that the hazard encountered by an infected wireless network, not only affects the security and privacy concerns, but also impedes the complex dynamics of the communications ecosystem. Consequently, the complexity and strength of security attacks have increased in the recent past making the detection or prevention of sabotage a global challenge.**

From the security and privacy perspectives, this paper presents a comprehensive detail on the core and enabling technologies, which are used to build the 5G security model; network softwarization security, PHY (Physical) layer security and 5G privacy concerns, among others. Additionally, the paper includes discussion on security monitoring and management of 5G networks. This paper also evaluates the related security measures and standards of core 5G technologies by resorting to different standardization bodies and provide a brief overview of 5G standardization security forces. Furthermore, the key projects of international significance, in line with the security concerns of 5G and beyond are also presented. Finally, a future directions and open challenges section has included to encourage future research.

***Index Terms*—Multi-access Edge Computing (MEC), Network Function Virtualization (NFV), Network Security, Network Slicing, Physical Layer Security (PLS), Privacy, Software-Defined Networking (SDN) and Telecommunication, 5G.**

I. Introduction

The evolution of mobile networks offered to satisfy the new demands for enhanced performance, portability, elasticity and energy efficiency of novel network services. 5G mobile networks adopt new networking concepts to further improve these features [1]. The telecommunication standardization bodies are working on integrating novel networking concepts such as Software Defined Networking (SDN), Network Function Virtualization (NFV), cloud computing, Multi-access Edge Computing (MEC), Network Slicing (NS) concepts to telecommunication networks [2], [3]. The target of such efforts is to design a new softwarized mobile network. It will help innovate and develop new network services to satisfy demand for the evolving the future mobile networks. The SDN concept proposes to decouple the control and data planes of networking devices [4]. The network control and intelligence of SDN based network are placed in a logically centralized controller. Moreover, it can offer an abstract of the underlying network infrastructure for the control functions and business application layer. NFV proposes a novel approach to create, deploy and manage networking services. This concept aims to decouple the network functions from proprietary hardware in order to run them as software instances [5]. Cloud computing and MEC will provide on demand scalability for the networks [6], [7]. Network slicing improves the support for different traffic classes in 5G Network [8]. Protecting the security and privacy have become the primary concerns in this new telecommunication networks as risks can have high consequences.

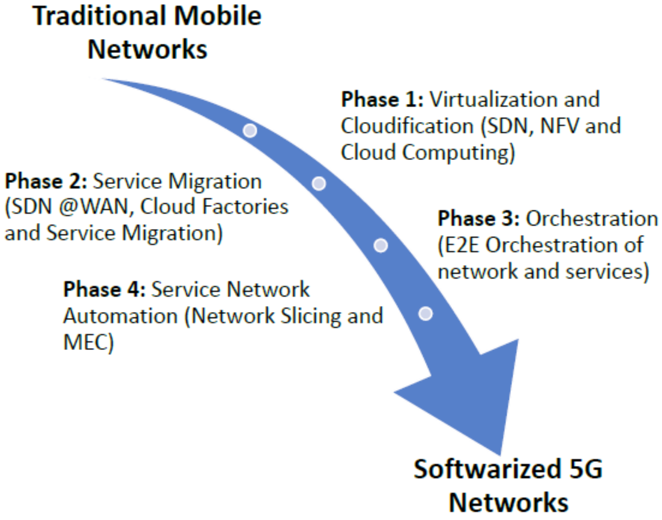

Traditional Mobile Networks
Phase 1: Virtualization and Cloudification (SDN, NFV and Cloud Computing)
Phase 2: Service Migration (SDN @WAN, Cloud Factories and Service Migration)
Phase 3: Orchestration (E2E Orchestration of network and services)
Phase 4: Service Network Automation (Network Slicing and MEC)
Softwarized 5G Networks

Fig. 1. Four phases of Network Transformation towards Network Softwarization in 5G.

Fig. 1 illustrates the four phases of network softwarization which paves the path towards 5G. It illustrates how above technologies has enabled the deployment of softwarized 5G network, spanning from inflexible fixed-mobile architecture

Rabia Khan is with the School of Computer Science and Robotics, National Research Tomsk Polytechnic University, Tomsk 634050, Russia. Email: khanrabia@tpu.ru

Pardeep Kumar is with the Department of Computer Science, Swansea University, Swansea, UK. Email: pardeep.kumar@swansea.ac.uk

Dushantha Nalin K. Jayakody is with Faculty of Engineering, Sri Lanka Technological Campus, Padukka 10500, Sri Lanka and School of Computer Science and Robotics, National Research Tomsk Polytechnic University, Tomsk 634050, Russia. Email: nalin@tpu.ru

Madhusanka Liyanage is with School of Computer Science, University College Dublin, Ireland and Centre for Wireless Communications, University of Oulu, Finland. Email: madhusanka@ucd.ie, madhusanka.liyanage@oulu.fi

*Corresponding author

TABLE I
SUMMARY OF MAIN ACRONYMS.

Acronym	Definition	Acronym	Definition
3GPP	Third Generation Partnership Project	5G	Fifth Generation Wireless Network
AI	Artificial Intelligence	AN	Artificial Noise
APT	Advanced Persistent Threats	AKA	Authentication and Key Agreement
ABE	Attribute Based Encryption	ARPF	Authentication Credential Repository and Processing function
ASON	Automatically Switched Optical Network	AUSF	Authentication Server Function
BS	Base Station	CJ	Cooperative Jamming
CR	Cognitive Radio	C-RAN	Cloud Radio Access Network
CSI	Channel State Information	DoS	Denial of Service
D2D	Device-to-device	DDoS	Distributed Denial of Service
DL	Down-link	DF	Decode Forward
DREAMS	Distributed Reputation Management System	ETSI	European Telecommunications Standards Institute
EST	Effective secrecy throughput	E2E	End-to-end
ECG	Electrocardiogram	EAP	Extensible Authentication Protocol
FDD	Frequency Division Duplex	FMEC	Fog and Mobile Edge Computing
GMPLS	Generalized Multi-protocol Label Switching	GDPR	General Data Privacy Regulation
HLPSL	High-level protocol specification Language	HW-PS	Hard-working path selection
HPN	High Power Node	HIP	Host Identity Protocol
HD	Half Duplex	HetNet	Heterogeneous Network
IIoT	Industrial Internet of Things	IoT	Internet of Things
ITU-T	International Telecommunication Union Telecom	IDS	Intrusion Detection System
ICT	Information and Communication Technology	IPWAVE	Internet Protocol Wireless Access in Vehicular Environments
IMSI	International Mobile Subscriber Identity	IETF	Internet Engineering Task Force
KFDP	Data based on Kalman filter	KPTSABE	Key-Policy Attribute-Based Encryption
LPN	Low Power node	LDP	Laplace mechanism for perturbed data
LTE	Long Term Evolution	LDPC	Low Density Parity Check Codes
LBS	Location Based Service	MitM	Man-in-the-middle
MANETs	Mobile Ad hoc NETworks	MRC	Maximum Ratio Combining
MIMO	Multiple Input Multiple Output	mmWave	Millimeter Wave
MEC	Mobile Edge Computing	MCC	Mobile Cloud Computing
MLT	Machine Learning Technique	MPWG	Mobile Platform Work Group
MRT	Maximal Ratio Transmission	MTC	Machine-type communication
MSN	Mobile Social Network	mmWave	millimeter Wave
mMTC	massive Machine Type Communication	NIST	National Institutes of Standards and Technology
NGMN	Next Generation Mobile Networks	NS2	Network Simulator Version 2
NS	Network Slicing	NOMA	Non Orthogonal Multiple Access
NVF	Network Function Virtualization	OFDMA	Orthogonal Frequency Division Multiple Access
ONF	Open Networking Foundation	PASER	Position-Aware Secure and Efficient mesh Routing
PBS	Pico Base Station	PLS	Physical Layer Security
P2P	Point to Point	QoS	Quality of Service
RA	Radio Access	RAN	Radio Access Network
RFC	Request For Comment	RS	Relay Station
SPA	Shortest Path Algorithm	SISO	Single Input Single Output
SDN	Software-Defined Networking	SDMN	Software-Defined Mobile Networking
SCP	sequential convex programming	SAF	Security Anchor Function
SHFRS	Soft Hesitant Fuzzy Rough Set	SIC	Successive Interference Cancellation
SDP	Semi-definite Programming	TDD	Time Division Duplex
SEAF	SEcurity Anchor Function	SERA	Secure Ergodic Resource Allocation
SRERA	Secure Robust Ergodic Resource Allocation	SEEM	Secrecy Energy Efficiency Maximization
SOP	Secrecy Outage Probability	SWIPT	Simultaneous Wireless Information and Power Transfer
SUPI	Subscription Concealed Identifier	SUPI	Subscription Permanent Identifier
TCG	Trusted Computing Group	UAV	Unmanned Ariel Vehicles
UDM	Unified Data Management	UE	User Equipment
URLLC	Ultra Reliable and Low Latency Communication	VEC	Vehicular Edge Computing
VNF	Virtual Network Functions	WSN	Wireless Sensor Networks
ZF	Zero Forcing	ZFBF	Zero Forcing Beamforming

to a dynamic and agile software based network architecture. These architectural changes in 5G are expected to fuel the digital transformation that all the industry is witnessing [9]. This will also result in generating new service models and new value chains which will lead to a significant socio-economic impact. The definitions of frequently used acronyms are presented in Table I.

Fig. 2 illustrates the high level architecture of 5G networks. The network softwarization enabled the ability to represent the 5G network as a layered model similar to SDN networks. Here, 5G will support a wide range of devices, including mobile phones and different IoT devices [10], [11]. IoT devices grow from simple household appliances to sensors and other high advanced technologies. Also, 5G will support different RAT (Radio Access Technologies) to connect these devices. In addition to the pre-4G radio, 5G will introduce a set of new radio technologies such as NOMA (Non-Orthogonal Multiple Access), massive MIMO, mmWave (millimeter Wave) and several other IoT communication technologies [12].

The backhaul of 5G network can be divided in to three different layers; Infrastructure layer, control layer and business application layer. The infrastructure layer contains the basic connectivity devices such as BS (Base Stations), routers and switches. In contrast to the pre-5G network, infrastructure layer devices do not enable with an intelligence. All the network control functionalities and decision making entities are placed in the control layer. This control layer interacts with the business layer. Also, it can translate the network service requests from the business layer as control commands and deliver to the infrastructure layer devices. Thus, all the network services as well as business applications are implemented in the business layer. In addition, The E2E (End to End) management and orchestration layer is used in parallel to synchronize the operation of all three layers.

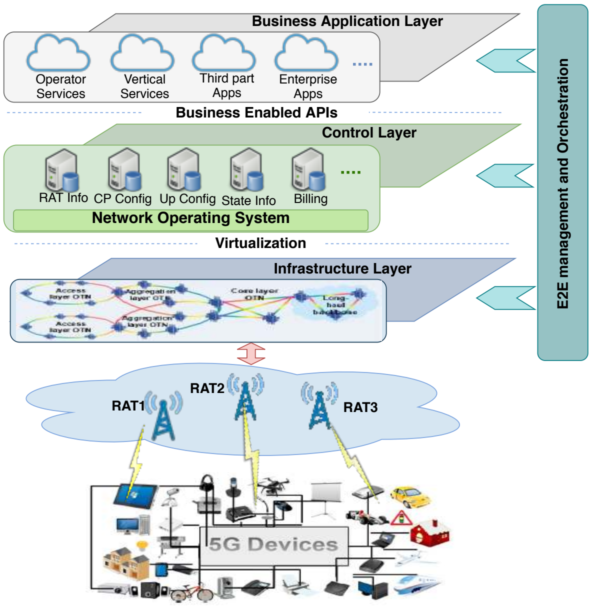


Fig. 2. The High level Architecture of 5G Network with different operational layers.

The security associated with 5G technologies has considered as one of the key requirements related to both 5G and beyond systems. Moreover, the most of the security models in pre-5G (i.e. 2G, 3G and 4G) networks can not be directly utilized in 5G due to new architecture and new services [13]. However, some of the security mechanisms can be used with some modification. For the backward compatibility with the previous generation, Open Air Interface (OAI) platform [14] discussed in the wide context of 5G and overview for the security protocol improvement in 5G provided in [15].

In the past, the key ambition for security in the telecommunication network was to ensure proper functionality of the billing system and the security of radio interface by encrypting the communication data. In 3G, two-way authentication is used to eliminate the connection establishment with fake BS. Finally, 4G networks use advanced cryptographic protocols for user authentication. It also offers the protection against the physical attacks such as the physical tampering of base stations, which can be installed on public and user premises. Moreover, some of the privacy issues were solved to a certain extent in pre-5G network since user data were stored in mobile operator own databases. However, 5G security and privacy issues are overpowering these mechanisms due to the change of architecture and new services.

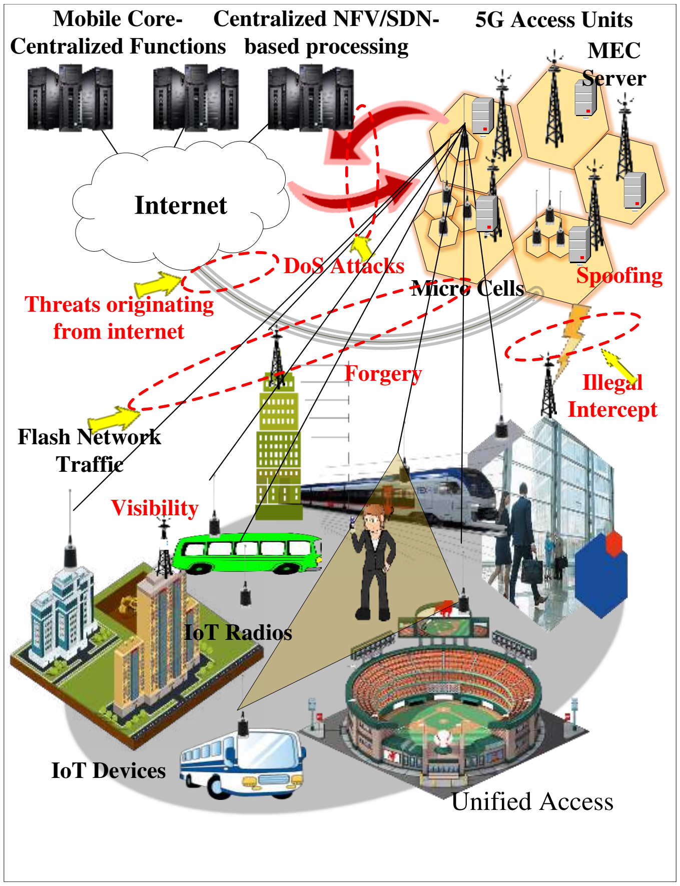


Fig. 3. The Overall View of 5G Security Impact for Heterogeneity of Connected Devices and More Users.

The security of 5G and beyond 5G networks has three main components. First, almost all the above security threats and security requirements related to pre-5G mobile generations are still applicable in 5G and beyond. Second, 5G will have a new set of security challenges due to the increased number of users, heterogeneity of connected devices, new network services, high user privacy concerns, new stakeholders and requirements to support IoT and mission-critical applications (Fig. 3). Third, network softwarization and utilization of new technologies such as SDN, NFV, MEC and NS will introduce a brand new set of security and privacy challenges. Fig. 4 illustrates the overall view of 5G Security requirements which has built based on these three components.

A. Motivation of the Paper and Comparison with Other Surveys

In this survey, we aim to provide an overview of the cutting-edge technologies (e.g., SDN, NFV, MEC, etc.) that are the main building blocks of 5G network. Another aim is to understand the security and privacy advances from the viewpoint of SDN, NFV, MEC, etc. To this aim, we mainly focus on the contributions from both academia and industry that are addressing security and privacy of 5G networks. As highlighted in Fig. 4, this survey has also focused on

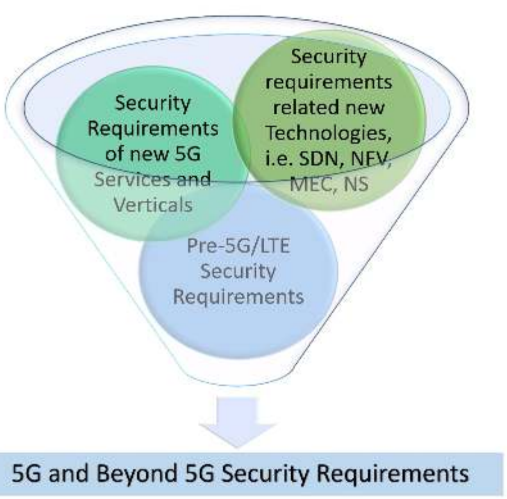

Security Requirements of new 5G Services and Verticals
Security requirements related new Technologies, i.e. SDN, NFV, MEC, NS
Pre-5G/LTE Security Requirements
5G and Beyond 5G Security Requirements

Fig. 4. Formation of 5G and Beyond Security Requirements

opportunities and challenges in terms of security which are related to key technologies in 5G.

As the next generation of mobile networks, 5G is one of the highly active research domains among telecommunication researchers. As a result several surveys were already published on 5G networks [1], [16]–[20]. Many future research possibilities such as architecture, mobility management, traffic management, security, privacy and techno-economic aspects, discussed in these papers which are highly important to be considered during the deployments of 5G networks. Among these requirements, the security of 5G core technologies network is an indefeasible factor. Security has highlighted as one of the utmost important requirements in 5G research domain. However, a quite limited number of survey papers were published in the 5G security domain [21]–[26]. None of the above surveys has considered all the aspects of the 5G security. A survey of existing authentication and privacy-preserving schemes from 4G to 5G are presented in [23]. However, the impact on 5G due to network softwarization techniques is still missing here. A survey on green communication and security challenges in 5G wireless communication networks was presented in [26]. A survey on security for 5G communications and SDMNs was presented in [24], [27], [28]. Since above papers were published in few years back most of the recent research works are not included. Moreover, 5G network softwarization techniques other than SDN and NFV were not considered.

On the other hand, 5G has developed on various novel network softwarization technologies such as SDN, NFV, MEC, cloud computing and NS. It is significant to consider the security of underline 5G technologies with analyses of the security in 5G networks. Table II summarizes the recently published surveys related to security of 5G and above 5G technologies. Most of these articles are focused on either individual technologies such as SDN, NFV, MEC and NS security. However, these studies are quite shallow in addressing security issues while integrating them in 5G networks.

Furthermore, in our previous research articles [21], [22], we briefly discuss the important of 5G security and the security challenges in underline technologies such as SDN, NFV and MEC. However, these papers do not contain a comprehensive analysis all the security aspects such as threat vectors, the security of network slicing and IoT as well as related projects. Thus, this survey offers a offer a comprehensive overview of the state-of-the-art security technologies and mechanisms which are required for the complementary security framework for 5G by extending the previous works.

B. *Our Contributions*

To the best of our knowledge there is not a single survey which addresses a broader range of 5G security by considering all of the key 5G technologies. Thus, this is the first work that considered security and privacy issues in the key network softwarization technologies used in 5G networks. Since all these network softwarization techniques are very essential to the realization of 5G, it is important to highlight their inter connection in terms of security and privacy. The main goal of this work is to broaden the horizons of potential inter-dependencies related to network security in different network softwarization technologies in the future 5G networks.

The contributions of our paper are listed below:

- **Study of security landscapes in 5G Networks:** A comprehensive search conducted on 5G security model, next generation threat landscape for 5G, IoT threat landscapes and threat analysis in 5G networks. In addition, the paper discusses the security recommendations, i.e., ITU-T and NGMN.
- **Identify the key areas of 5G security, from the state-of-the-art literature:** The paper discusses in detail various security challenges related to key areas of 5G security.
- **Highlight the security challenges related to key technologies in 5G** Identify and discuss the open challenges and opportunities in security and privacy related to the key 5G technologies, i.e. SDN, NFV, MEC, cloud computing and network slicing.
- **PLS (Physical Layer Security) in 5G:** The PLS section contains a discussion on the current hot research areas in 5G physical layer communication network. For each research area we presented our contribution in both tabular and graphical forms.
- **Investigate security monitoring and management in 5G network:** The future networks will connect a huge number of devices, which will exponentially increase the security issues in monitoring and management of 5G networks. Therefore, we examine the security issues and countermeasures in 5G network monitoring and management.
- **Comprehensive view of privacy in 5G networks:** The paper categorizes the privacy from the viewpoint of users and identify privacy challenges for the 5G networks. Furthermore, the paper pointed out a few regulatory objectives in privacy protections and privacy mechanisms in the 5G networks.
- **Discuss activities in standardization bodies:** The role of different standardization bodies is utmost important to

TABLE II
SUMMARY OF IMPORTANT SURVEYS RELATED TO 5G SECURITY

Aspect	Ref.	Main contribution	Relevance to 5G Security
5G General	[1]	A comprehensive overview on the new architectural changes proposed for Radio Access Network (RAN) design for 5G.	No explicit focus on security aspects.
	[18]	A review on the vision of the 5G networks by discussing architectural options, application implementation issues as well as real demonstrations and testbeds.	Describes the Security and privacy issues and management related to UEs (User Equipment), access networks, D2D communication and C-RAN.
	[19]	A comprehensive survey of on different 5G backhaul network technologies and solutions.	No explicit focus on security aspects.
	[20]	A survey of latest research and development effort related to 5G.	No explicit focus on security aspects.
5G Security	[21], [22]	Highlight the security and privacy threats in 5G networks and the possible security solutions for these threats.	Discuss the security challenges related to SDN, NFV, mobile clouds technologies and possible 5G privacy issues.
	[23]	A survey of existing authentication and privacy-preserving schemes for 4G and 5G mobile networks.	Presents a classification of threat models in 4G and 5G cellular networks in four types of attacks, i.e. attacks against privacy, integrity, availability, and authentication. Also provides a classification of three countermeasures, i.e. cryptography methods, humans factors, and intrusion detection methods.
	[26]	A survey on green communication and security challenges in 5G networks.	Possible security attacks on users within the Small Cell Access point (SCA) of the 5G networks have studied.
	[29]	A A survey on the Security and the evolution of Osmotic and Catalytic Computing for 5G Networks.	Highlight the use of recent computing paradigms as alternative mechanisms for the enhancement of 5G security.
General Mobile network Security	[30]	A survey on existing literature on attacks and defenses in all three pre-5G network generations.	Explore relevant security and privacy threats in pre-5G mobile networks and discuss the potential impact on 5G networks. No implicit focus on impact of new 5G technologies.
SDMN Security	[25]	A survey of SDMN and its related security problems.	Explore relevant security threats and their corresponding countermeasures with respect to the data layer, control layer, application layer, and communication protocols in SDMNs.
	[27]	A survey on issues and challenges in designing SDN based wireless networks.	Review various SDN based seminal security solutions for 4G and 5G.
	[28]	A review on security enhancement in SDN based wireless networks.	Discuss how SDN can used to enhance the security of SDMNs.
SDN Security	[31]–[34]	A survey of related security issues in SDN based systems.	No explicit focus on 5G and security aspects of other 5G technologies.
NFV Security	[35]–[37]	A survey of related security issues in NFV based systems.	No explicit focus on 5G and security aspects of other 5G technologies.
IoT Security	[38]–[45]	A survey of related security issues in IoT.	No explicit focus on 5G and security aspects of 5G technologies.
	[46], [47]	A survey of using novel technologies such as machine learning and blockchain to enhance the security in IoT.	No explicit focus on 5G and security aspects of 5G technologies.
	[48]	Discussion with respect to Perception, Network, Middle and Application layers	Threats and solutions for upcoming 5G challenges.
	[49]	A survey for all IoT layers, specific discussion on applications, network architecture and industrial trends.	Analyze security, privacy and proposed a security model for risk minimization.
Access control and Privacy	[50]	A survey for a host centric network with Physical, Network and Application layers.	Focus on existing access control, security and privacy mechanism.
SDN security	[51]	Discuss SDN security and data plane programmability security implications for SDN to stateful SDN.	Enlightened vulnerabilities with their reduced exposure and stateful SDN Data planes security.
Physical Layer Security (PLS)	[52]	AN injection, anti-eavesdropping signal design, prevented beamforming/precoding, secure cooperative transmission, resource allocation and controlled power approach has been reviewed.	Emphasis that cryptography is not applicable for 5G.
	[53]	Discussion on three different approaches: Spatial modeling, mobile association and device connection for HetNet.	No explicit focus on 5G and security aspects of 5G technologies.
	[54]	Discussion the importance of PLS for secure transmission of information in 5G	A short survey focusing only on PLS.
D2D communication	[55]	A survey that emphasised that Application layer is mostly based on cryptography. The approach of D2D taxonomy and better layer combination security protocol has been used.	PLS can be tackled without cryptography.
Control plane ASON	[56]	A survey of related security issues in the structure, functions, protocols, security analysis and probable attacks in 5G technology.	Concludes that ASON is a potential solution for increasing network growth.

define the security of 5G network. The paper contains a discussion on the security standards from different standardization bodies and a brief overview of the roles of different 5G standardization security forces.

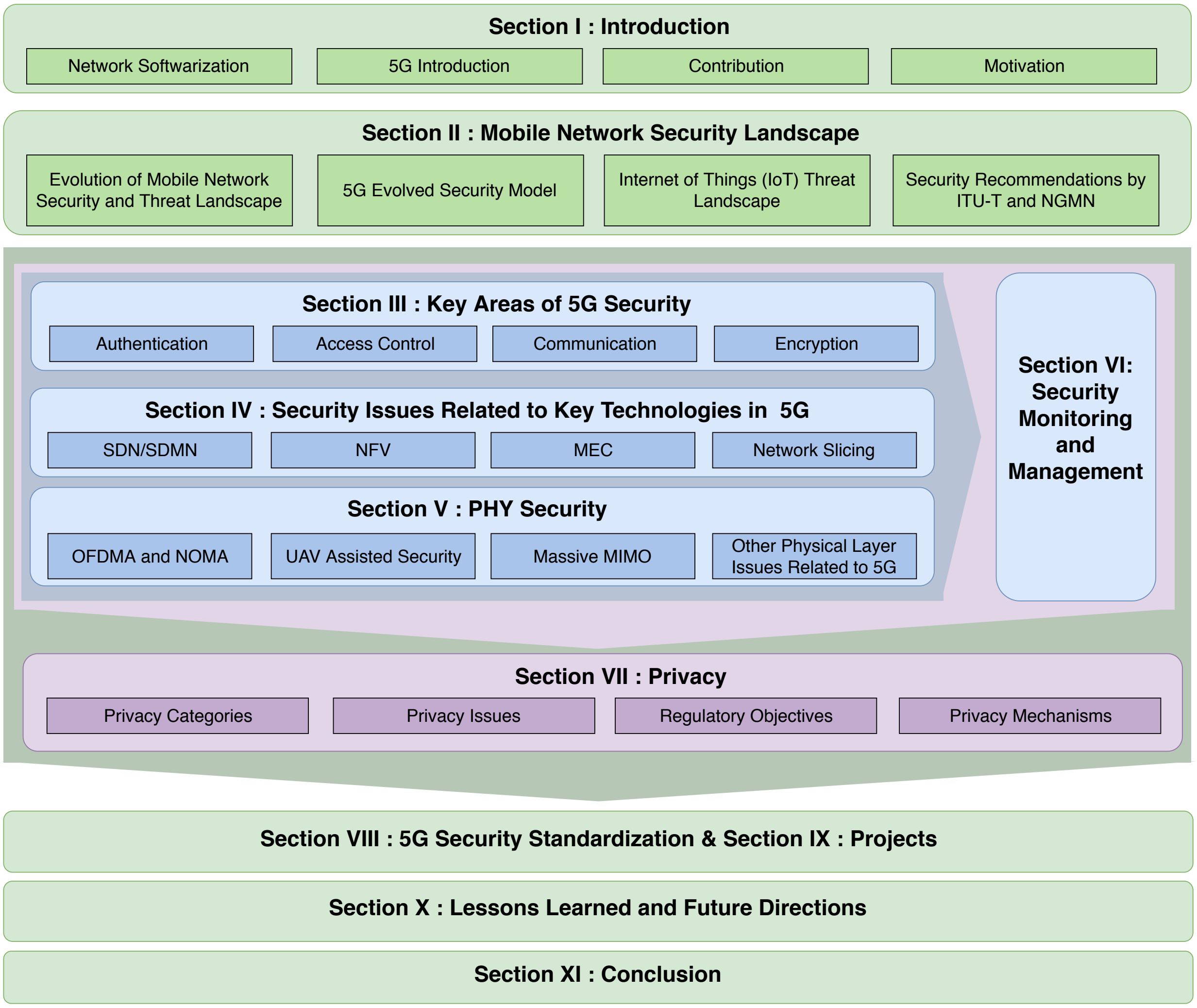

Section I : Introduction
Network Softwarization
5G Introduction
Contribution
Motivation
Section II : Mobile Network Security Landscape
Evolution of Mobile Network Security and Threat Landscape
5G Evolved Security Model
Internet of Things (IoT) Threat Landscape
Security Recommendations by ITU-T and NGMN
Section III : Key Areas of 5G Security
Authentication
Access Control
Communication
Encryption
Section IV : Security Issues Related to Key Technologies in 5G
SDN/SDMN
NFV
MEC
Network Slicing
Section V : PHY Security
OFDMA and NOMA
UAV Assisted Security
Massive MIMO
Other Physical Layer Issues Related to 5G
Section VI: Security Monitoring and Management
Section VII : Privacy
Privacy Categories
Privacy Issues
Regulatory Objectives
Privacy Mechanisms
Section VIII : 5G Security Standardization & Section IX : Projects
Section X : Lessons Learned and Future Directions
Section XI : Conclusion

Fig. 5. The Outline of the Paper

- **Present holistic overview on ongoing research projects in 5G security.** The paper discusses various intentionally signified ongoing research projects globally, those are addressing and contributing efforts to 5G security.
- **Future research directions:** Based on our finding, we have highlighted the possible and important research challenges that have to be addressed, along with their early solutions and future directions. This helps future researchers to find their future directions.

C. Outline of the Paper

The rest of the paper is organized as follows: Section II presents the mobile network threat landscape. It includes the discussion about security evolution from 1G to 4G, 5G evolved security model, 5G threat landscape, IoT threat landscape, 5G threat analysis and the 5G security recommendations by different telecommunication standard organizations. Section III is particularly focuses on the key areas of 5G security. It presents security issues related to authentication, access control, communication security and encryption. Each key area is described with its security requirements for 5G and related works. Section IV is particularly focuses on security issues related to the key 5G technologies, i.e. SDN/SDMN, NFV, MEC, cloud computing and network slicing. Security issues associated with with each of these technologies are extensively discussed. Moreover, the relevance to the 5G security is also presented with related works. Section V presents a current hot research areas in 5G physical layer security. The main focus of this section is to discuss security in the OFDMA (Orthogonal Frequency-Division Multiple Access), NOMA, UAV (Unmanned Aerial Vehicle), mmWave, massive MIMO, channel coding, RF (Radio Frequency) energy harvesting and other physical layer issues related to 5G. Section VI discusses the security monitoring and management aspects of 5G networks. It presents the existing challenges in 5G security monitoring and management as well as the related work on the domain. Section VII contains a complete discussion of 5G privacy. Section VIII discusses the network security related activities in various standardization bodies in 5G eco-system. Section IX summarizes the proceeding research projects in the 5G security domain. Based on our findings, Section X describes the lessons learned and future research directions. Finally, Section XI concludes the paper. The outline of the paper has illustrated in the Fig. 5.

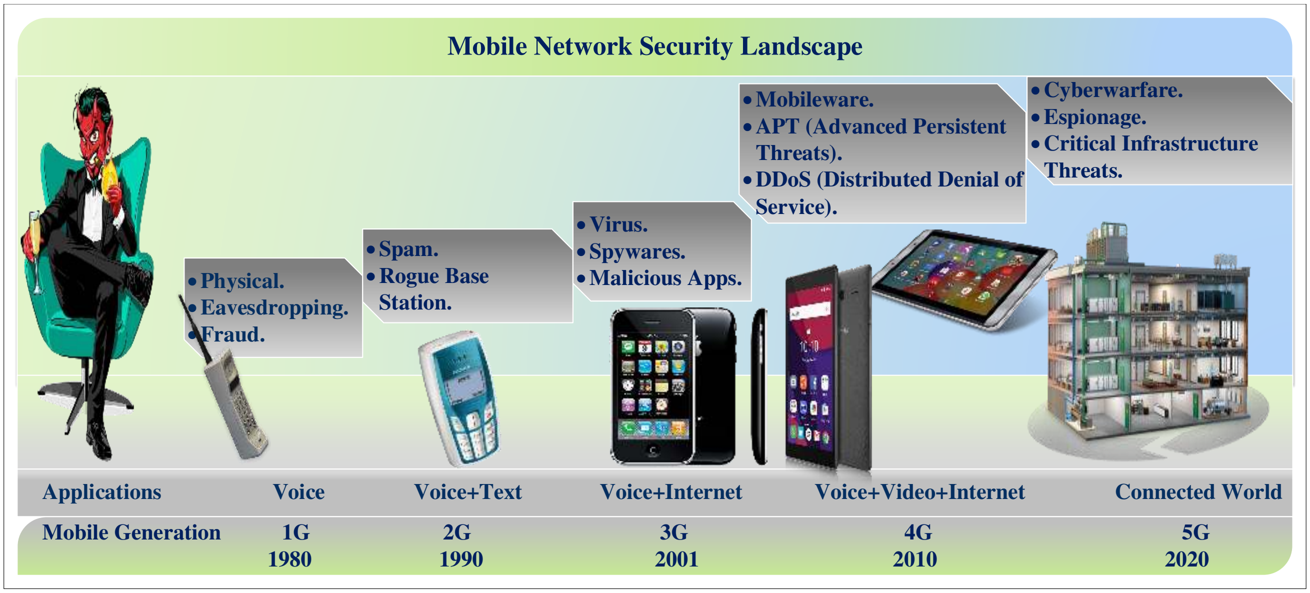


Fig. 6. Evolution of Mobile Network Security Landscape with offered technologies and respective security threats.

II. Mobile Networks Security Landscape

This section provides the basic landscape for the overall 5G security communication system. The entire evolved security model is discussed with general threat landscape, IoT threat landscape, 5G security threat analysis, and security recommendation by ITU-T, and NGMN are also presented in this section.

A. Evolution of Mobile Network Security and Threat Landscape

The telecommunication networks have evolved through four generations and we are at the edge of experiencing the latest 5G mobile networks. Along with each mobile generation, the security landscape of mobile networks has also evolved. The evolution of mobile network security landscape is presented in the Fig. 6.

In the early 1970s, the telephone networks were vulnerable only for the phreaking or hacking threats [57], [58]. In the modern era, technology has taken a twist drastically. Telecommunication has shown up a radical change to an info-communication system. Evolution of technology occurred parallel to the increment of security threats. It has been progressed from a war dialer to worms, viruses and modern-day APTs (Advanced Persistent Threats) [3]. Challengingly, protection tools have also evolved in the form of anti-virus, physical access control, context-aware firewalls, and modern application as discussed in [3].

1) 1G Security and Threat Landscape: The very first mobile network or 1G mobile network were introduced in 1980s [59]. It was based on analog technologies. 1G mobile phones were able to support only voice call services within a single country. 1G mobile networks were also known Advanced Mobile Phone System (AMPS) in United States (US) and the Nordic Mobile Telephony (NMT) in Europe. Data services and roaming were not a part of 1G mobile network service list. However, mobile security threats begin with the introduction of 1G mobile communication. With the passage of time, technology grew dynamically and provided a challenging threat landscape. The hacking was easier in 1G mobile network since it's radio link had no support for encryption due to their analog nature. Therefore, the 1G calls can be easily intercepted. If the attacker wants to intercept a call, he just has to use a radio scanner and tune it to the correct frequency. By intercepting these calls, the attacker can obtain the user credentials such as the Mobile Identification Number (MIN) and Electronic Serial Number (ESN). Later, these credentials can be used to clone another phone to impersonate the subscriber.

Later, evolved 1G networks supported optional analog scrambling to prevent attackers listening to the channel. Although, these scrambling methods were able to prevent such scanning issues, it was not strong as encrypted methods used in later mobile generations.

2) 2G Security and Threat Landscape: After 1G mobile communication, 2G mobile networks were introduced in 1991. 2G provided voice plus messaging facility for the mobile users. It was the first mobile generations to introduce data services, i.e.SMS (Short Message Service). Moreover, 2G networks were operated in digital domain [60]. 2G network introduces several security features such as authentication of subscribers using shared-secret cryptography, the encryption of radio interface traffic and protecting the confidentiality of the subscriber's identity. 2G networks used SIM (Subscriber Identity Module) card; which a hardware security module which stores a cryptovariable. This has to use in each mobile phone and it verifies the identity of the mobile subscriber.

2G was also suffered by a unique set of security challenges. In 2G networks, attackers were using spamming as pervasive attacks for transmitting unwanted information to the users. It resulted in a number of spam messages in users' mobile. Attackers used spam messages for vicious purposes. Interruption of mobile communication with fake authentication of rogue

BSs was one of the introduced hacking process [61], [62].

Moreover, both stream ciphers, i.e. A5/1 and A5/2 used in 2G networks to encrypt the calls can break realtime by using a ciphertext-only attack [62]. SMS also had security vulnerabilities due to its store-and-forward nature. Especially, the content of roaming SMS messages were exposed to external attackers who reside within the Internet [63].

3) 3G Security and Threat Landscape: Mobile phones were fulfilling basic ICT requirements of human life. Such observation motivated mobile researchers to introduce data applications and Internet in 3G mobile communication technology. NTT DoCoMo launched the first commercial 3G network on 2001, using the Wideband Code Division Multiple Access WCDMA technology by enabling mobile Internet access. Initially, bandwidth of 3G network is 128 Kbps for mobile stations, and 2 Mbps for fixed applications [64]. Later 3G network versions were able to support high data rates and new services such as video call, MMS (Multimedia Message Services), mobile television and mobile internet.

Lessons learned from 2G security issues were helped to design better security mechanisms in 3G networks. The key security issues in 2G networks such as false BS attack and shorter key lengths, were corrected in 3G. Moreover, 3G security features and mechanisms were designed in a way that they can be can be extended and enhanced to mitigate new threats and satisfy the security requirements on new services [62].

Furthermore, 3G security architecture consisted of five different sets of features, i.e 1) network access security, 2) network domain security, 3) user domain security, 4) application security and 5) visibility and configurability of security [62].

3G mobile communication system cellular phones also faced a lot of security threats which targeted the operating system, user phones, and the computer system. Vulnerability of the mobiles caused malicious code gain to unauthorized access which includes users' sensitive information. 3G networks were also vulnerable to attacks such as eavesdropping, impersonation of a subscriber, user impersonation with compromised authentication vector, impersonation of the network, man-in-the-middle attacks, denial of service attacks by de-registration spoofing, location update spoofing and camping on a false BS.

4) 4G Security and Threat Landscape: It was the first time for 4G-LTE (Long Term Evolution) that all mobile devices switched to E2E (End to End) architecture based on all-IP. 4G was deployed in 2010 and early 4G networks supports speed up to 100 Mbps. Use of a higher Layer Protocol (IP) as transport medium affords intelligence at every stage within the network relative to a service.

The security architecture of 4G builds upon the lessons learned from deploying the 2G and 3G networks. 4G introduced a new set of cryptographic algorithms and a significantly different key structure than 2G and 3G. New cryptographic algorithms such as EPS Encryption Algorithms (EEA) and EPS Integrity Algorithms (EIA) were used 4G [62]. Moreover, most of the keys in 4G are 256-bits long in contrast to the 128 bit keys in 3G. Moreover, 4G uses different algorithms and key sizes for the control and user planes traffic. The primary 4G authentication mechanism is known as the Authentication and. Key Agreement (AKA) protocol and use of AKA required by 3GPP TS 33.401 [65]. Here, integrity and replay protection for 4G air interface traffic are provided by NAS (Non-Access Stratum) and RRC (Radio Resource Control)-signaling protocol. After that, the 4G backhaul traffic should be encrypted by using IPsec protocols [66].

The open all-IP based 4G architecture becomes vulnerable to various security attacks. Due the coherent IP connectivity of 4G core network with the Internet, 4G networks becomes vulnerable to millions of attackers and new security threats from the Internet [62] [67]. 4G networks are now vulnerable a large set of IP based attacks such as IP address spoofing, TCP SYN DoS, User ID theft, Theft of Service (ToS), DoS (Denial of Service), and intrusion attacks [67]. Moreover, pre-4G networks had some level natural protection due to the use of none IP protocols in the core network [68]. It makes the job of attackers very difficult. Understanding the complex mobile protocols was difficult for the attackers. The IP core has relaxed this hurdle in 4G [23] [69].

In addition, new high power 4G mobile devices are perfects sources to perform DoS, Botnet, APT, viruses and worms. Moreover, 4G networks support multiple non-3GPP networks such as Wi-Fi and WIMAX [67]. Thus, 4G will inherit all the security problems of these networks as well. Comparably, non-3GPP networks such as Wi-Fi and WIMAX have lower levels of security than a mobile network [23], [68]

With the new 4G technology mobile operators were capable of providing new offers including high speed of the services. However, it also increased the impact of security challenges. APT and DDoS (Distributed Denial of Service) are greatly affecting the system security and leaded to high financial losses. Attackers become organized and wiser than expectation. Some of these attacks became harder to detect the presence of an attack in IP based 4G mobile network [23], [68].

5) 5G Threat Landscape: 5G is offering a mind-blowing improvement in the network services. It will allow billions of devices to operate with better reliability, facilities, speed, system capacity, bandwidth utilization, fault tolerance and latency than 4G devices. 5G era will provide an ideal target for attackers due to IoT, connected world and critical infrastructure facilities as shown in Fig. 3 and 7. High probability of attacks is especially toward political and financial motivated gains by criminals and professionals with extensive resources and knowledge of technology. 5G threat landscape dynamically based on complex and sophisticated threats like flame and stuxnet malwares. A brief overview on 5G evolved threats can be observed from Fig. 7. The rest of the sections are presented with the detailed descriptions of threat landscape of 5G.

B. 5G Evolved Security Model

Wireless communication systems are not only limited to typical phone audio and video calls. They also support a number of applications including gaming, shopping, social networking, Bring Your Own Device (BYOD), home appliances, and cloud technologies which have opened up wide range of research challenge to developers [20] [70].

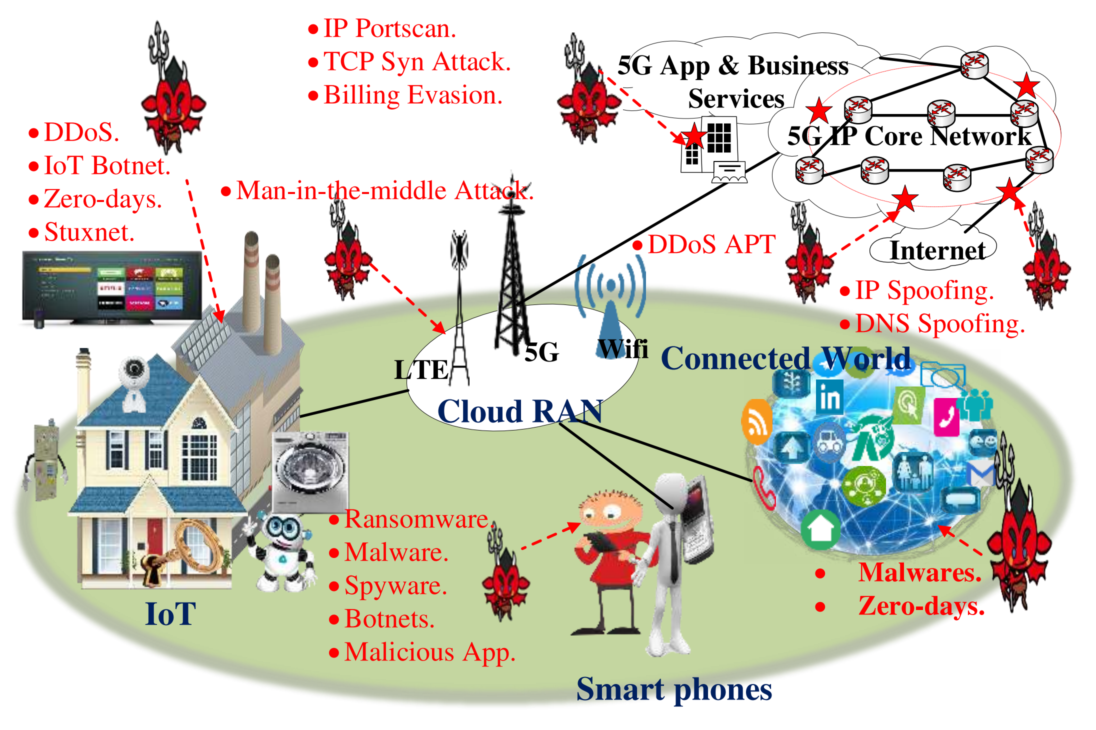


Fig. 7. 5G Security Threat Landscape for several attacks in IoT, smart phones, cloud RAN and connected world.

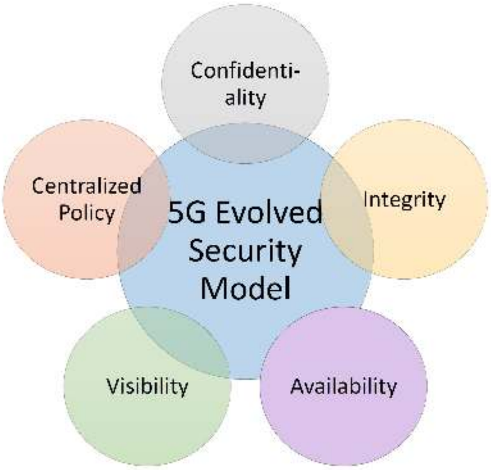


Fig. 8. 5G Evolved Security Model for upcoming technology's threat awareness.

Similarly, phreaking is not limited to stealing general information [58]. It has now converted into big cyber-crime rings with clear financial, political and personal motives [71]. The IoT world has now brought another big challenge where the connection between the devices is opening a number of vulnerabilities within the 5G network [41]. Therefore, provision of adequate security level is mandatory for the ever-evolving security threat landscape of 5G communication. Following [57], [72], the authors have integrated visibility and centralized policy as two new security parameters in the conventional Confidentiality, Integrity and Availability (CIA) for enhancing security and protection of users' data as shown in Fig. 8.

1) Confidentiality: In the 5G security model, data confidentiality is one of the main security requirements; the property that can protect data transmission from disclosure to unauthorized entities and from passive attacks (i.e., eavesdropping). Considering the 4G-LTE and 5G architectures, any user plane data must be confidential and protected from unauthorized users [73]. Standard data encryption algorithms have been widely adopted to realize the data confidentiality in 5G network applications (e.g., vehicle network [74], health monitoring [75] etc). The symmetric key encryption algorithm can be utilized to encrypt and decrypt 5G data with one private key. This is shared between the communicating entities (e.g., a sender and a receiver).

2) Integrity: This is to prevent tempering and loss of information during transformation from one point to another. Integrity of 5G New Radio (NR) traffic is protected similar to 4G. In 5G NR, the integrity protected of wireless data traffic at the Packet Data Convergence Protocol (PDCP) layer. In 4G LTE integrity protection is provided only for Non-Access Stratum (NAS) and Access Stratum (AS) [82]. However, One main of key advancement in 5G integrity protection entails that 5G NR offers the integrity protection of the user plane as well. This is significant because 4G did not support the integrity protection of the user plane. This new feature is useful for small data transmissions, particularly for constrained IoT devices. Moreover, 5G authentication mechanism 5G-AKA is using integrity-protected signaling. This ensures that no unauthorized party can modify or access the information that is communicated over the air [83].

3) Availability: In 5G domain, networks availability is to ensure that the network resources can be accessible when-

TABLE III
IoT Security Challenges and Solutions.

Ref	Technology	Challenge/Threat	Solutions	Layers	Protocols
[76]	IoT Smart water system	●Cyber-attacks. ●Epidemic attack. ●Faults and destructive attack. ● Security and Privatized Security.	●ABA-IDS algorithm	●Applications. ●Perception/end devices. ●Services. ●Communications.	●Wi-Fi. ●ETHE(Ethernet).
[77]	IoT security component	●Authentication. ●Authorization.	●OAuth 2.0-based oneM2M component	● Perceptions.	●CoAP. ●MQTT.
[78]	General IoT	●Eavesdropper collusion.	●PLS.	●Communications.	●blacktooth. ●ZigBee. ●IEEE. 802.15.4
[79]	IoT environment	●Dolev-Yao threat.	●Signature-based AKA scheme.	●Communication.	● HLPSL
[80]	SDN based IoT-Fog	●MitM	●Blood filter method	●Perception	●OpenFlow
[81]	Industrial Mobile-IoT	●Malware.	●Dynamic, static, and hybrid analysis.	●Android applications.	

ever they are needed by legitimate users, since the availability effects on the reputation of service provider. In another words, the availability ensures the high probability effectiveness of network infrastructure. It also measures the sustainability of a network against active attacks, e.g., DoS attack. A DoS attack can degrade the network performance. However, in [84], the authors suggested that via the extreme Mobile Broadband (eMBB) and ultra-reliable Machine-Type-Communication (uMTC) the network availability can be achieved by at least 95% and 99.99%, respectively, for the 5G applications.

4) Centralized security policy: In 5G network, the current 3GPP 4G security architectures cannot directly applied to the new 5G use-cases as they are dedicated to the traditional operators-subscriber trust model. Therefore, to support new innovations (such as NFV and SDN), there is the need for a centralized security policies management system that provides convenience for users to access the applications and resources. In [85], Thanh et al. proposed a policy-based security management framework (VISECO) to support centralized security management for 5G. The authors claimed that with the help of VISECO, mobile operators can secure their network infrastructure. In addition, the operators can enable Security-as-a-Service (SaaS) as a potential solution to several customers such as IoT vendors.

5) Visibility: Visibility enables E2E-awareness of mobile networks to the control plane. This can efficiently tackle the basic network issues to ensure a secure environment. The 5G networks need to utilize comprehensive end-to-end security strategies, which should cover all layers of the network including application, signaling and data planes. To implement such comprehensive security mechanism, 5G operators should have a complete visibility, inspection and controls over all layers in the network. Here, the 5G technologies should be integrated with open APIs to manage with the security policies. In such a way, 5G network can have consistent security polices of both software and hardware in the network. The enhanced visibility across the network and security policies will help to implement contextual security mechanisms which is suitable for new 5G services. Moreover, enhance visibility enables data-driven threat prevention to find and isolate the infected devices before attacks can potentially take place.

C. Threat Landscape of Internet of Things (IoT)

Recently, IoT has drawn a great attention due to the attractive and unique features. The idea is to provide a smart world built on the combination of millions of smart computing devices. Several offered smart applications services including Social IoT (SIoT), Industrial IoT (IIoT), IoT-fog, IoT smart water system, health care IoT and smart grids [86], [87]. With the drastic increase in the web of the technology, the risk of security threats and challenges are also increasing rapidly. Not only the technology but also threats are getting smarter. This problem immediately needs to be resolved. Table III shows some of the detected threats with their proposed solutions. Moreover, Fig. 9 illustrates the threat landscape on different IoT applications.

Several researchers have provided solutions to the detected threats in different domains of IoT. Due to high density and low latency requirements, the solutions of security issues for IoT networks are challenging. However, the authors of [81] analyzed the security threats and detection schemes of the industrial IoT networks statistically, dynamically and with hybrid detection. This analysis is particularly helpful for the application designers. In [88], the authors analyzed threats for PLS and industrial IoT environment. Suggestion for abundant PHY-Sec (Physical Layer security) technologies in [89] provides assistance for enhanced industrial wireless system security.

By introducing a viable attack model in an IoT-Fog architecture, the authors of [80] have investigated the possible threats of MitM attacks on the Open-Flow control channel in the SDN based IoT-fog systems. In [90], authors have studied SIoT security landscape by providing a taxonomic analysis from transportation, perception and application level perspective. In IoT smart water system, the authors of [76] have proposed a procedure to develop a threat model ABA-IDS (Abnormal Behavior Analysis-Intrusion Detection System) for identifying attacks against four layers including; services, devices, communication and application layers. As a part of

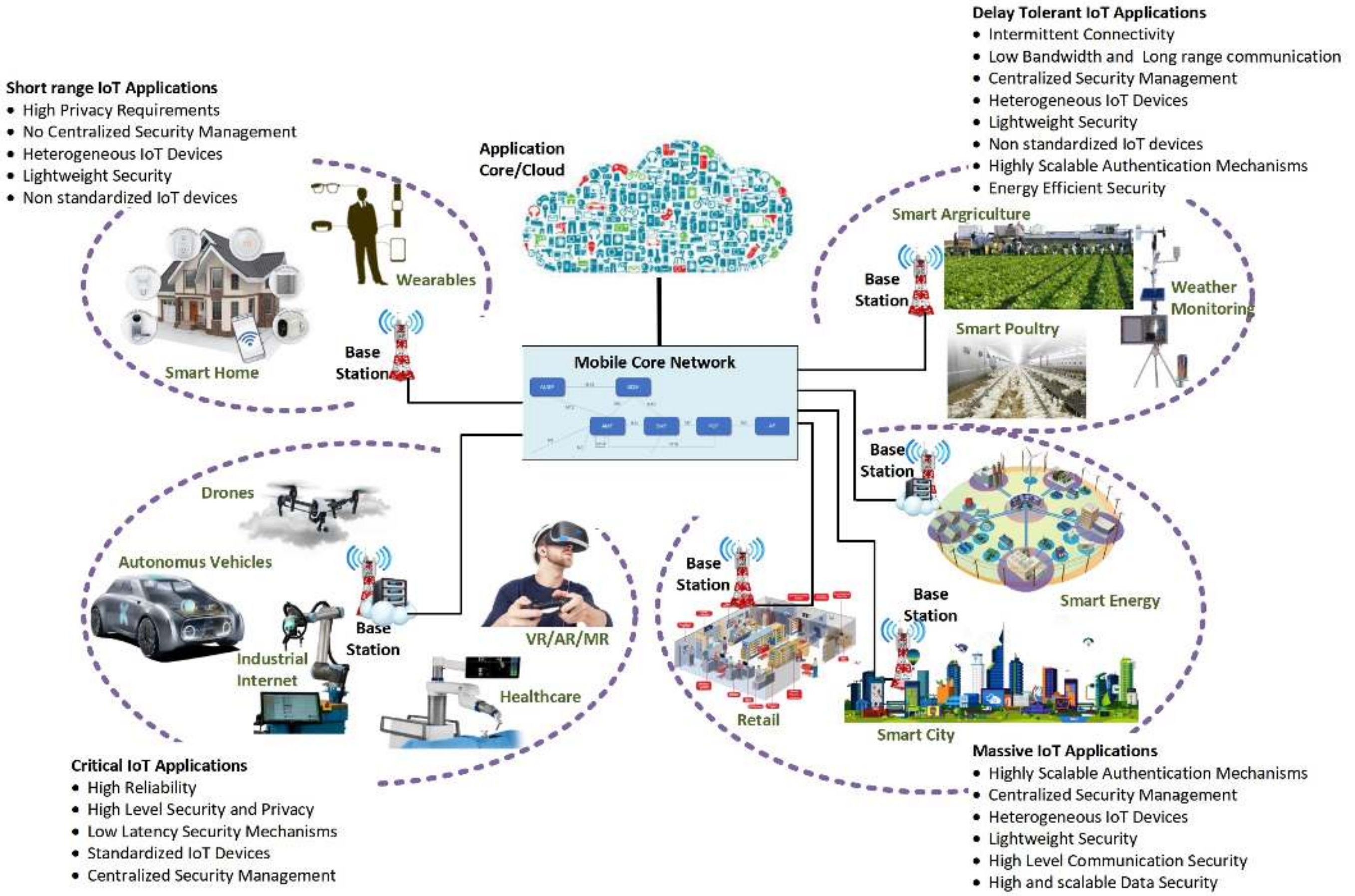

Delay Tolerant IoT Applications
• Intermittent Connectivity
• Low Bandwidth and Long range communication
• Centralized Security Management
• Heterogeneous IoT Devices
• Lightweight Security
• Non standardized IoT devices
• Highly Scalable Authentication Mechanisms
• Energy Efficient Security
Short range IoT Applications
• High Privacy Requirements
• No Centralized Security Management
• Heterogeneous IoT Devices
• Lightweight Security
• Non standardized IoT devices
Application Core/Cloud
Wearables
Smart Home
Base Station
Mobile Core Network
Smart Argriculture
Base Station
Weather Monitoring
Smart Poultry
Base Station
Drones
Autonomus Vehicles
Industrial Internet
Base Station
VR/AR/MR
Healthcare
Base Station
Retail
Base Station
Smart Energy
Smart City
Critical IoT Applications
• High Reliability
• High Level Security and Privacy
• Low Latency Security Mechanisms
• Standardized IoT Devices
• Centralized Security Management
Massive IoT Applications
• Highly Scalable Authentication Mechanisms
• Centralized Security Management
• Heterogeneous IoT Devices
• Lightweight Security
• High Level Communication Security
• High and scalable Data Security

Fig. 9. Threat landscape on different IoT categories and their applications.

the communication layer, the authors have presented the way to use the proposed model for protecting the secure gateway. This model is capable of detecting known and unknown attacks with a high detection rate.

For the prediction of ventricular arrhythmia, the authors of [91] have developed a secure and ultra-low power IoT sensing platform. The authors development uses signals of ECG to get a chip-specific ECG key for enabling the protection of the communication channel. The proposed scheme when implemented with an existing design provides hardware level protection as well.

Keeping the importance of authentication in mind, the authors of [79] have proposed an authenticated key establishment scheme based on signatures for IoT. The proposed scheme is comparable to some of other techniques and verified for security by resorting to Burrows-Abadi-Needham logic, formal and informal security analysis via automated validation of application tools and internet security protocol. To scale proportionately solutions for the issues of confidentiality, trust and privacy in distributed networks, the authors [92] provided a novel configurable policy-based specification and analyzed vulnerabilities and threats of IoT system.

A few authors have provided the security threats solutions in terms of hardware components of the IoT system environment. For addressing the security challenges at the perception layer, the authors of [93] targeted the common security issues of IoT and system hardware. Authors have given some of the security features to incorporate in the System on Chip (SoC)/micro-controllers for achieving the target. In [77], authors claims to fulfill the requirement of the required security component in IoT by proposing OAuth 2.0-based oneM2M for providing authentication and authorization. In [94], the authors have proposed a reconfigurable cryptographic processor called Recryptor. It uses near-memory and in-memory computing for supporting cryptographic large vector calculations efficiently. Various secret/public key cryptographies and hash functions for the implementation of cryptographic primitives have been utilized.

According to [95], along with the set of opportunities, IoT integration with integrated 5G depends highly on large-scale deployed sensors, which increase the security risk drastically. For better data streaming, private Unscented Kalman filter (UKF) has proposed for both linear and non-linear systems, which ensures the privacy of user's data collected by the cloud. For the evaluation of private streaming data based on Unscented Kalman Filter (UKFDP), four real world data set and average relative error has taken. The authors of [78], used PLS and analytical approaches including classical probability theory, Laplace transform, and Cauchy integral Theorem for analyzing secrecy outage probability of an IoT system.

D. Security Recommendations by ITU-T

This subsection discusses the security properties, which are basically recommended by the ITU-T. These security properties can address several aspects of the ICT systems, applications, services and information in 5G domain, as follows.

- *Access Control*: Access control mechanisms prevent the malicious use of a resource, including the prevention of use of a resource in an illegal manner. Typically, these mechanisms (e.g., role-based access control) ensure that only legitimate users, devices or machines are granted permissions (e.g., read, write, etc.) the resources in a network, database, information flows, services and applications.
- *Data confidentiality*: In a 5G network, many devices collect and forward sensitive data to many stakeholders. Therefore, data confidentiality protects data from unauthorized disclosure and ensures that the authorized users can read the data content.
- *Data integrity*: Integrity property ensures the data is not modified in the transit or data is intact from its source to the destination.
- *Authentication*: Entity authentication is a mechanism that is used for one entity to prove its identity to a corresponding entity. An authentication mechanism can protect from impersonation threats.
- *Network availability*: It ensures that network is always available in normal and even in disaster recovery operations. Events impacting the network, such as device failures, natural disasters and security compromise, the network must available to the users and devices.
- *Non-repudiation*: This property is used to demonstrate that the origin of the received data or messages is a particular peer. This peer cannot falsely deny the authenticity of the data or message as the message is signed by the peer's private key.

E. Security Threats and Recommendations by NGMN

Technological improvements are bringing dynamic changes to the system architecture and network requirements. Due to a number of connected devices in 5G communications, there is a high probability of new security threats. According to the demands and requirements of system security NGMN has provided some of the probable threats with recommendations for their solutions [96]–[99]. Table IV lists out the possible security threats and their recommendations by NGMN.

For the most of the security threats, NGMN has either recommended the explosion of new mechanism or authentication for network slicing, access network, MEC, latency and consistent user experience.

III. KEY AREAS OF 5G SECURITY

This section presents the most challenging security issues related to the key security areas in 5G, i.e, access control, authentication, communication and encryption.

A. Authentication

Authentication plays a significant security role in any communication system to verifying the identity of users. Numerous techniques had used for authentication in each generation of mobile communication. However, this section is enlightening the authentication technique particularly developed for 5G communication system by 3GPP. Preliminary there is a basic division of authentication; primary and secondary authentication. The 3GPP completed the normative specifications of 5G Phase 1 in 3GPP Release 15. Fig. 10 demands the authentication in 5G Phase 1 security. Primary authentication provides device and network mutual authentication in both 4G and 5G. However, due to evolved 5G nature, primary authentication has also evolved minor differences. Built-in home control authentication mechanism controls the knowledge and call of device authentication. 5G-AKA and Extensible Authentication Protocol (EAP)-AKA are two mandatory authentication selections for 5G phase 1. Specific cases such as private networks are optionally allowing EAP based authentication. Primary authentication can run over non-3GPP technologies as well since it is independent of the RA (Radio Access) technology. The authentication of data networks outside a mobile operators domain is secondary authentication. EAP based associated credentials and authentication methods are applicable to this method.

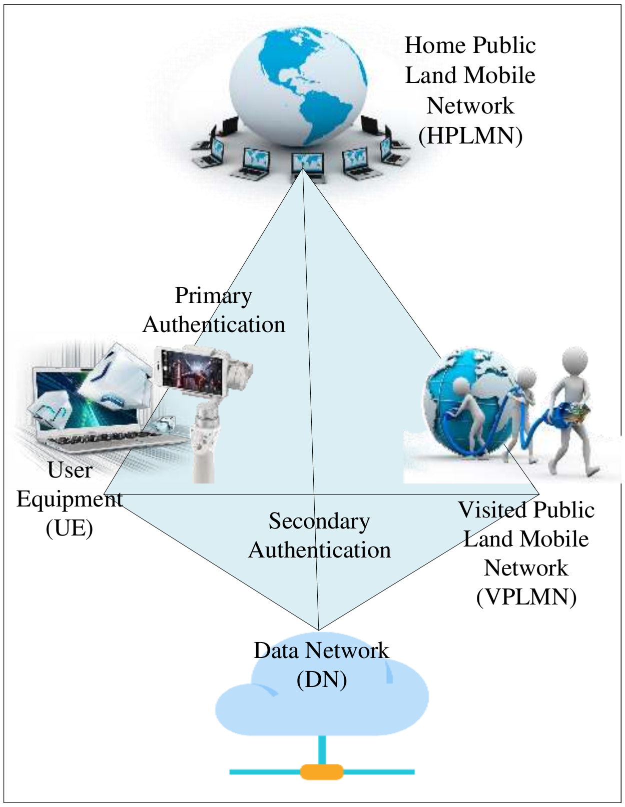


Fig. 10. Authentication in 5G Phase 1 security enhancement.

Mutual authentication and the provision of keying material between the UE and the network are achievable with key management and primary authentication procedures. The primary key and authentication management procedures provide an

TABLE IV
SECURITY THREATS AND RECOMMENDATIONS BY NGMN [96]–[99]

Domain	Threats	Recommendations
Network Slicing	Communication between inter-network slices is not secure.	Controlled and secure communication between all slices, function and interfaces between them.
	Impersonation attack against physical host platform and network slice manager.	Mutual authentication between host platform and network slice manager.
	Within an operator network impersonation attack against a Network Slice instance.	Authenticity and integrity of Network Slice instance need to be verified.
	Within an operator network impersonation attack against multiple Network Slice Managers.	Mutual authentication between all Network Slice Managers.
	Variance of policies and protocols for different slices.	Proper isolation between slices and separate authentication of each slice for a UE or authentication at a lower security slice.
	Denial of service attack to other slices.	Capping for slices individually for provisioning maximum resources.
	Affect of other slices' resources exhaustion.	Ring-fencing provide flexibility to run in all conditions.
	Side channel attacks due to same set of primary hardware.	Avoid co-hosting with different level of sensitivity and strong isolation of virtual machines.
	Combination of vitualized and regular function in a hybrid deployment model offers new threats.	Maintenance of same 5G security level.
	Service for UE with multiple slices at the same time provides risk of security.	Sealing between slices with a security mechanism in both UE and network.
Access Network	Expected high traffic either malicious or accidental.	Reduce traffic changers whenever possible and be flexible for maintaining system performance.
	Risk of key leakage between operator's links.	Strong security link between operators or a new method for key sharing.
	Optional security implementation offers security threat.	Study for mandating security.
	Subscriber device level security in 5G due to roaming routed IP traffic in 5G.	Virtualization and network slicing.
DoS Attack	Exhaustion of signaling plane with a number of devices that gain access simultaneously.	Stop new unknown access through access control when network is exhausted or check the novelty and standardization of signal patter and requires to find a new method to overcome DOS attack.
	Exhaustion of signaling plane with a number of simultaneously and intermittently data transfer devices.	Avoid time synchronized data transfer, Use of analytical techniques for consistent and persistent communication devices, access control and designing of new techniques.
	Stopping services for a number of devices due to traffic overload is sometimes a trick by an attacker.	Series of overload defenses, defense overload mechanism and designing of new mechanism that limits services for the problematic devices.
	Bulk configuration leading to bulk provisioning.	Analytical techniques like anomaly detection.
MEC	MEC deployment billing risk.	Periodic polling from UE to core network to cross check received charging records from edge. A new or similar mechanism like that of 3GPP.
	MEC applications run on the same platform of network function.	A new framework for either providing access to only trusted MEC devices or making MEC and network operator independent of trust.
	Influence on network by an allowed third party.	Network operators must limit network distortion to a certain level.
	Providing security service to a third party.	Expose security services to trusted applications only.
	MEC environment user plane attacks.	It is required to carefully study the scenario specially in case of a number of caches and new architecture.
	Sensitive security assets on Edge.	Proper encryption, assurance of security, protection of decryption keys.
	Exchange of data between Edge and Core.	Encryption of the sensitive asset.
	Trust establishment between the edge and the core functions.	Authentication between communication resources.
	MEC Orchestrator communication security.	Guarantee of the security level as per recognized scheme.
	Multiple new nodes, RD and many LI points will raise security risk.	Follow strong physical security and identified method of implementation and location for LI/RD functionality.
Latency	Security mechanism for latency targets.	Changes in 3GPP architecture, moving encryption operation to lower layer, dropped user plane security, use a fast stream cipher.
	Subscriber authentication within visited network.	Re-use of old SA (Security Association) for low latency at user plane and high latency at signalling plane and Delegating DSS (Distributed Subscriber Server) from HSS (Home Subscriber Server) to visited network by a key "Ki" for subscribers' authentication.
	Re-authentication request for the loss of service on a user plane.	No critical path on user plane and no strict bound between user plane and control plane.
Consistent User Experience	Credentials to IMS (Internet protocol Multimedia Subsystem) and 3GPP network access.	Prevent credentials at required level of security.
	Access for non-3GPP network.	Authentication, key agreement, if untrusted access then set up authentication process between UE and the core.
	Weak security for less trusted 3GPP network access.	Security must be provide by home network between UE and core network.
	Secure interfaces between UE and non-3GPP radio access points.	UEs and 3GPP servers must have the capability to derive the credential and to mannage these credentials.

anchor key known as KSEAF. Authentication Server Function (AUSF) of home network provides KSEAF for the SEAF of the network server. According to 3GPP and ETSI, the Network Function (NF) and AUSF provides authentication of

UE for NF petitioner in 5G core network. It allows Access and Mobility Management Function (AMF) to the NF service consumer for authenticating UE. NF provides UEs identity and serving network name to AUSF to perform the authentication. Now AUSF uses the information provided by AMF for 5G-AKA or EAP-based authentication. Fig. 11 and 12 show the authentication mechanism for 5G-AKA and EAP-based authentication with EAP-AKA method.

Recently different authors investigated 5G security threat mechanism for different threats and scenarios. In [100], authors perform a formal analysis of 5G AKA protocol, provided precise requirements from the 3GPP 5G standards and highlighted the missing security goals. For the authentication of BS, in [101] an algorithm fulfills the requirement in existing 5G authentication protocol. The work of [102] provided analysis over 5G-AKA. It revealed the dependency of 5G-AKA on the underlying channels. A revival of attack against 5G AKA protocol, exploits the vulnerability of devices in [103]. Authors of [104], have presented a review on 4G and 5G AKA vulnerabilities with realization of Authentication Authorization and Accounting (AAA) weaknesses. In [105] authors have shown the compatibility of existing Universal Subscriber Identity Module (USIM) with perfect secrecy 5G AKA protocol. According to the heterogeneous 5G network requirement, authors of [106] have proposed an advanced group based AKA threat model. Authors of [107] showed that except IMSI-catcher attack, all identified attacks against 5G-AKA are still applicable and provided a modified version of 5G-AKA for respective prevention.

Braeken et al. proposed a novel 5G authentication and key agreement protocol in [108]. The authors utilized random numbers, which reduced the communication costs and provided robust security. The proposed scheme exploited the asymmetric key encryption to encyrpt the SUPI and generates a message SUCI. Note that here SUCI is a log-in request. Then the log-in request is verified by the home network. Moreover, the authors claimed that the usage of random numbers for 5G AKA protocol is possible since the current Universal Subscriber Identity Modules (USIMs) are now capable of performing randomized asymmetric encryption operations. In addition, their proposal is secure against post-compromise security and forward security. In another work, Ozhelvaci-Ma proposed a secure vertical handover authentication for 5G HetNets in [109]. This scheme provides a secure and seamless handover mechanism to supply strong, quick and mutual authentication. The authors proposed to use Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) that utilized a certificate-based scheme. In a similar vein, Ma-Hu proposed a cross layer collaborative handover authentication for 5G network [110]. The main idea of this scheme is to use the cross-layer (i.e., physical layer) and then utilize the EAP-AKA authentication to provide more secure and reliable services to the user. The authors adopted nonparametric Kolmogorov-Smirnov (K-S) test to perform the physical layer authentication.

Considering the backdrop of the 5G security model, authors of [111] have proposed 4G+RAM authentication model which depends on 4G plus frequency-based re-authentication protocol (4G+FRP) and 4G plus relative authentication model (4G+RAM). In [112] authors proposed Privacy-Preserving Authentication (PPAKA-HAMC) and Key Agreement protocol (PPAKA-IBS) for an anonymous and secure D2D group communication. In [113] authors proposed an AKA scheme based on IoT notion for heterogeneous WSNs for mutual authentication, anonymity and several other types of attack.

B. Access Control

The main purpose of access control is performed selective restriction of the access to the network. Access control networks have controlled by the network providers to provide a secure and safe network environment. It is the main building block for any type of network security system. The access control environment only confirms the authentic users' access to the system. Fig. 14 depicts a secured access control system with the basic security features. Access control strategies indicated at an extraordinary implementation independent level of concept and then imposed onto the real system by influencing accessible policy application mechanisms. In some of the latest access control systems, the decentralization of the network improves the secure environment of the network system. In [120], an access selection scheme has been proposed for D2D PLS along with multiple eavesdroppers. In the proposed scheme, with respect to distance thresholds, D2D communication devices are sharing spectrum with cellular users. The authors generated interference used by the authors to misguide eavesdroppers through jamming. Optimal throughput achievement of access selection scheme optimized the security level from eavesdroppers. D2D protection pair is used to protect a single user.

In [121], automated ConfigSynth framework has been proposed to provide affordable and synthesizing precise network configuration. The proposed framework is further refined to provide improved security by developing a refinement mechanism. The proposed algorithm provides isolation, distribution of security devices and better traffic flow. For prevention from International Mobile Subscriber Identity (IMSI) downgrade attack with a fake LTE BS, [122] provided the use of existing pseudonym-based solution and a mechanism to update LTE pseudonyms. Realizing the paging protocol security issues, an attack called ToRPEDO is explored in [101].

A number of proposed techniques for access control based on encryption, authentication and secret sharing have been offered by multiple authors. In [123], Accountable and Privacy-Enhanced Access Control (APAC) has been proposed to ensure user privacy. The authors also authenticate the validity of the protocol by implementing on limited experimental resources. In [124], authors have proposed a unique authentication scheme with biometric and password for Telecare Medicine Information System (TMIS). The proposed technique provides forward secrecy, anonymity, less computational cost and efficient authentication without involving remote server. In [125], authors proposed to expand the existing state of the art of management and policy specification by developing formal verification scheme for access control policies. Based on the update of ciphertext and computation outsourcing in

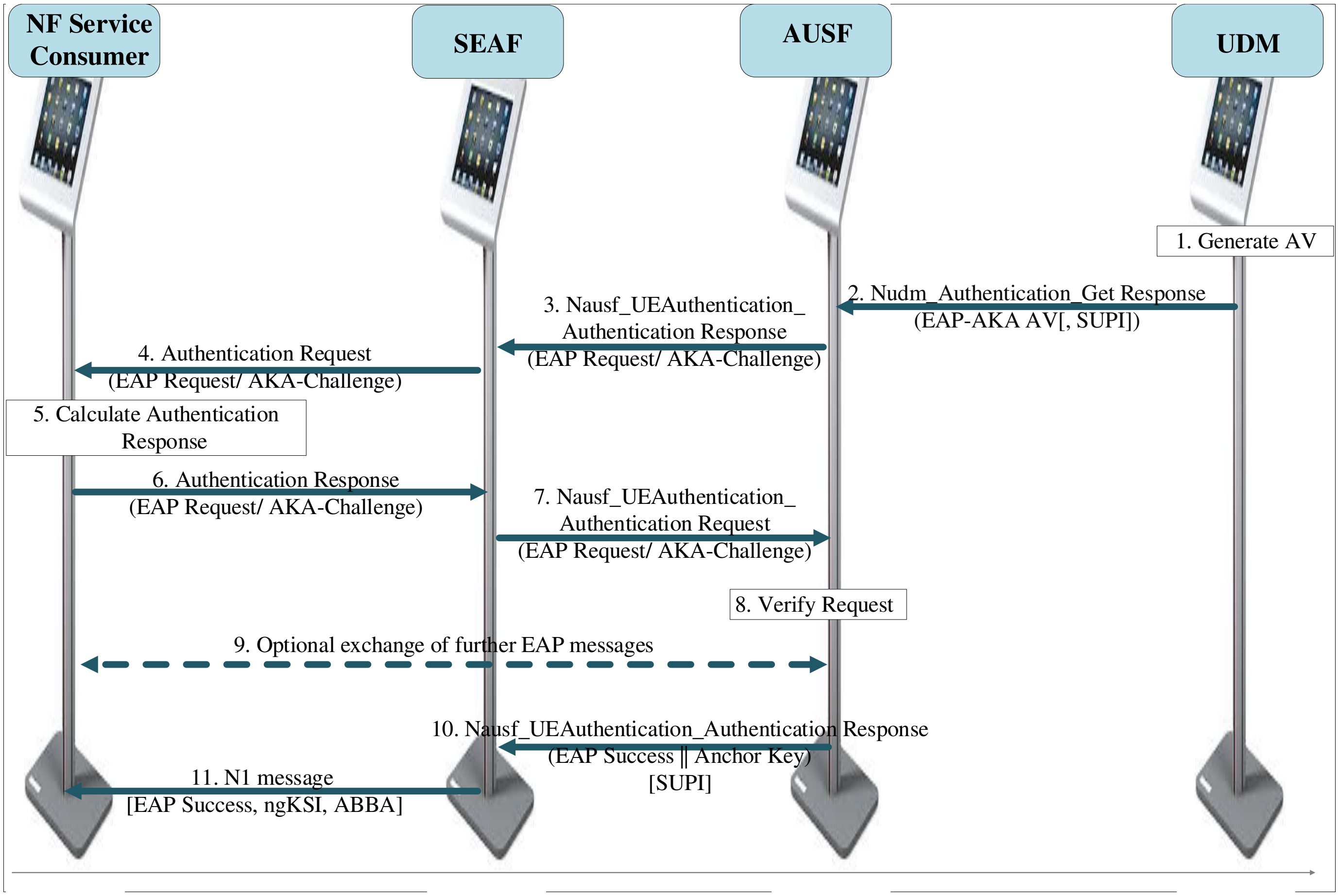

NF Service Consumer
SEAF
AUSF
UDM
1. Generate AV
2. Nudm_Authentication_Get Response (EAP-AKA AV[, SUPI])
3. Nausf_UEAuthentication_ Authentication Response (EAP Request/ AKA-Challenge)
4. Authentication Request (EAP Request/ AKA-Challenge)
5. Calculate Authentication Response
6. Authentication Response (EAP Request/ AKA-Challenge)
7. Nausf_UEAuthentication_ Authentication Request (EAP Request/ AKA-Challenge)
8. Verify Request
9. Optional exchange of further EAP messages
10. Nausf_UEAuthentication_Authentication Response (EAP Success || Anchor Key) [SUPI]
11. N1 message [EAP Success, ngKSI, ABBA]

Fig. 11. EAP Based Authentication Scheme with EAP AKA Method.

fog computing for IoT, authors of [126] proposed an access control scheme. User's data is encrypted using ABE and then feed into cloud storage. A secure and efficient security scheme has been offered in [127]. Based on Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE) and secret sharing, security data sharing scheme for multiple users in Online Social Networks (OSNs) has been proposed. In [127], authors have also proposed a partial decryption construction to reduce computation overhead of users by delegating decryption operations to OSNs, check ability mechanism to cross check decrypted data by OSNs, attribute revocation method for achieving backward and forward secrecy.

In [128], a node admission protocol BiAC (Bivariate polynomial secret sharing) is proposed using a temporary and secured MANET using a bivariate polynomial. The proposed protocol is a non-interactive, efficient and secure admission technique for secure sharing. To decentralized the system, MANETs are allowed to share secretly and efficiently pairwise secret keys without being assisted by any centralized support. They have also proposed a technique through which on-the-fly secure communication channel can be established by the pair of MANET nodes. In [129], a generalized hierarchical access control scheme called Shared Encryption Based construction (SEBC) has identified by adding qualified users to the system via perfect secret sharing and symmetric encryption. The proposed protocol defines alternative methods of accessing the system and it allows the distribution of duties to different users. It also construct a secure key assignment schemes called Threshold Broadcast Encryption Based Construction (TBEBC), in this scheme encryption bases on public key threshold broadcast.

Unique characteristics of ad-hoc networks allow the vulnerability of the system largely. In the form of ad hoc network groups, access control to the system plays the fundamental role. It prevents the access of intruder individual or group to the system. In [130], authors have proposed an attack on the famous Robust Access Control (RSA) proactive signature scheme. According to authors, RSA scheme leaks some information which has been utilized by the intruders to rebuild the entire shared secret. Multiple-Input Single-Output (MISO) relay cooperative scheme for a near and a far vehicle has been studied in [131].Cooperative Jamming (CJ), protected zero techniques and signal superposition has been adopted through which near user decodes its signal and acts as a relay for far user. Optimal secure transmission scheme has proposed after careful analysis for eavesdropping security threats. In the Downlink (DL) practical scenario with Channel Estimation (CE) errors for C-RAN systems with optimal Remote Radio Heads (RRHs), authors of [132] have investigated the reliability and security performance. Authors of [133] have

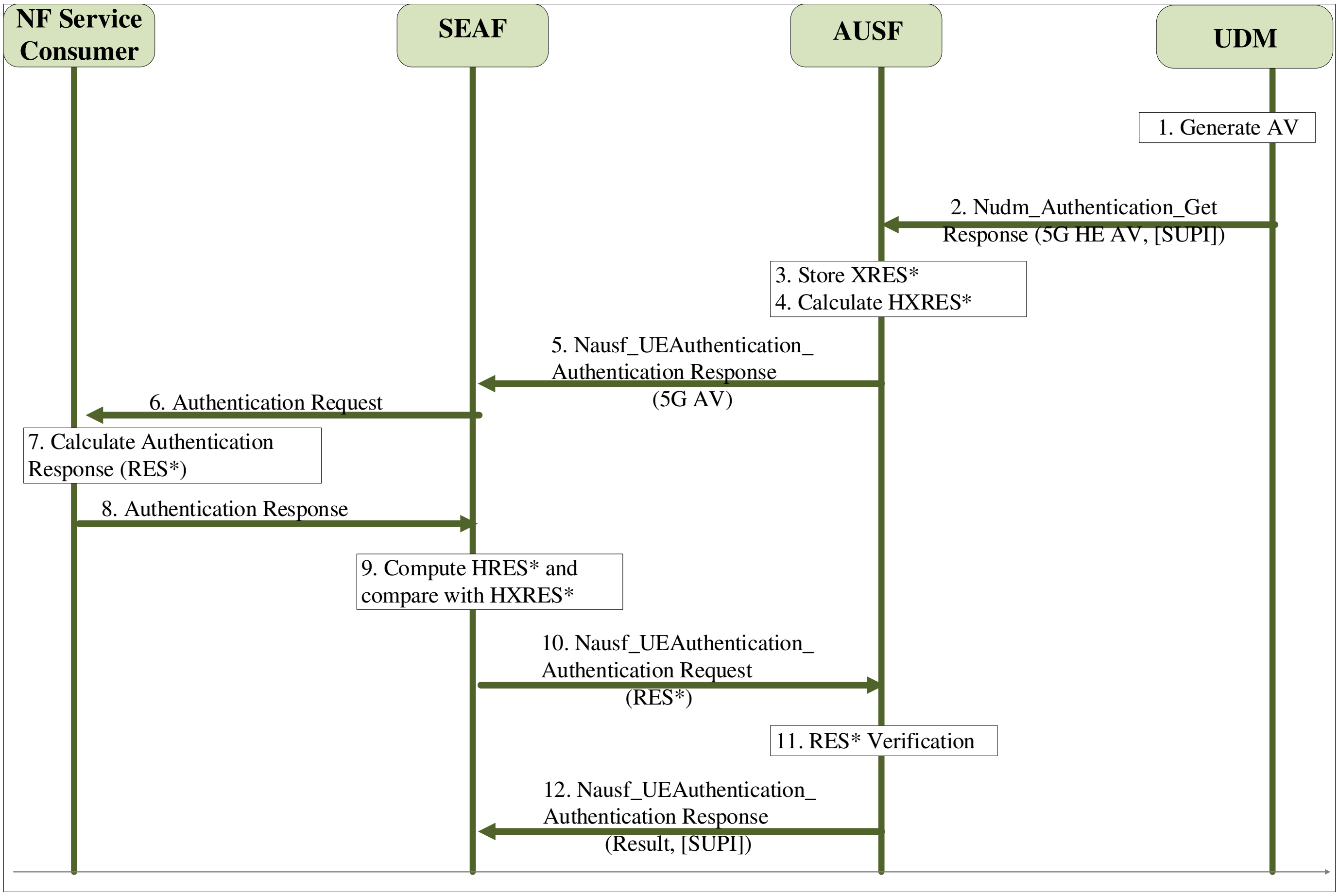

NF Service Consumer
SEAF
AUSF
UDM
1. Generate AV
2. Nudm_Authentication_Get Response (5G HE AV, [SUPI])
3. Store XRES*
4. Calculate HXRES*
5. Nausf_UEAuthentication_ Authentication Response (5G AV)
6. Authentication Request
7. Calculate Authentication Response (RES*)
8. Authentication Response
9. Compute HRES* and compare with HXRES*
10. Nausf_UEAuthentication_ Authentication Request (RES*)
11. RES* Verification
12. Nausf_UEAuthentication_ Authentication Response (Result, [SUPI])

Fig. 12. 5G Authentication and Key Agreement scheme.

proposed a new methodology for performing semiautomatic verification for implementation of access control policy in Industrial Network Systems (INS). Authors used a twofold model approach with consideration of two different system views including the detailed description of the target physical scheme and the abstract requirement of access control policies. Precisely, authors in [133], used high-level implementation framework called Role-Based Access Control (RBAC) for defining the policies.

Moreover, roaming events can happen very frequently in the 5G network due the utilization of local 5G networks or micro 5G operators [134]–[136]. Most of these local 5G operators do not have a high level of security similar to the main MNOs. Therefore, it is highly probable to encounter with a malicious local 5G network as a serving network [108]. Therefore, 5G authentication should be strong enough to avoid the connection establishment with such networks.

C. Communication Security

5G communications aim at providing high data bandwidth, low latency communication and extensive signal coverage to support a wide range of verticals in 5G Eco system. Therefore, 5G communication will be updated along with the architectural changes and integration of new technologies. However, these changes can lead also to tremendous security challenges in the future 5G mobile networks [137].

Attacks on 5G communication can be initiated at the different segments such as UEs, the access networks and the mobile operators core network [138]. To help understand the future security issues and challenges affecting on 5G communication, Table V summarizes the attacks related to different segments of 5G communication. It is also important to explore threats and attacks on legacy mobile systems (i.e., 2G/3G/4G). Some of these attacks are still applicable in 5G systems as well [3]. Fig. 13 is illustrates the impacting point of each security issues in 5G communication channel.

The 5G core network traffic can be classified in to two types, i.e. control traffic and user data traffic. Both these traffic types are vulnerable to different security threats. The key security issue related to the control traffic is the lack of IP level security. In the existing SDN based 5G core network, higher layer (application layer) security protocols such as Transport Layer Security (TLS)/ Secure Sockets Layer (SSL) sessions are used to secure the control channel communication. They have known IP level vulnerabilities such as IP spoofing, message modification attacks, eavesdropping attacks, TCP SYN DoS, IP spoofing and TCP reset attacks [119]. Therefore, it is necessary to use IP level security mechanisms along with higher layer protection mechanisms. In [21], [72],

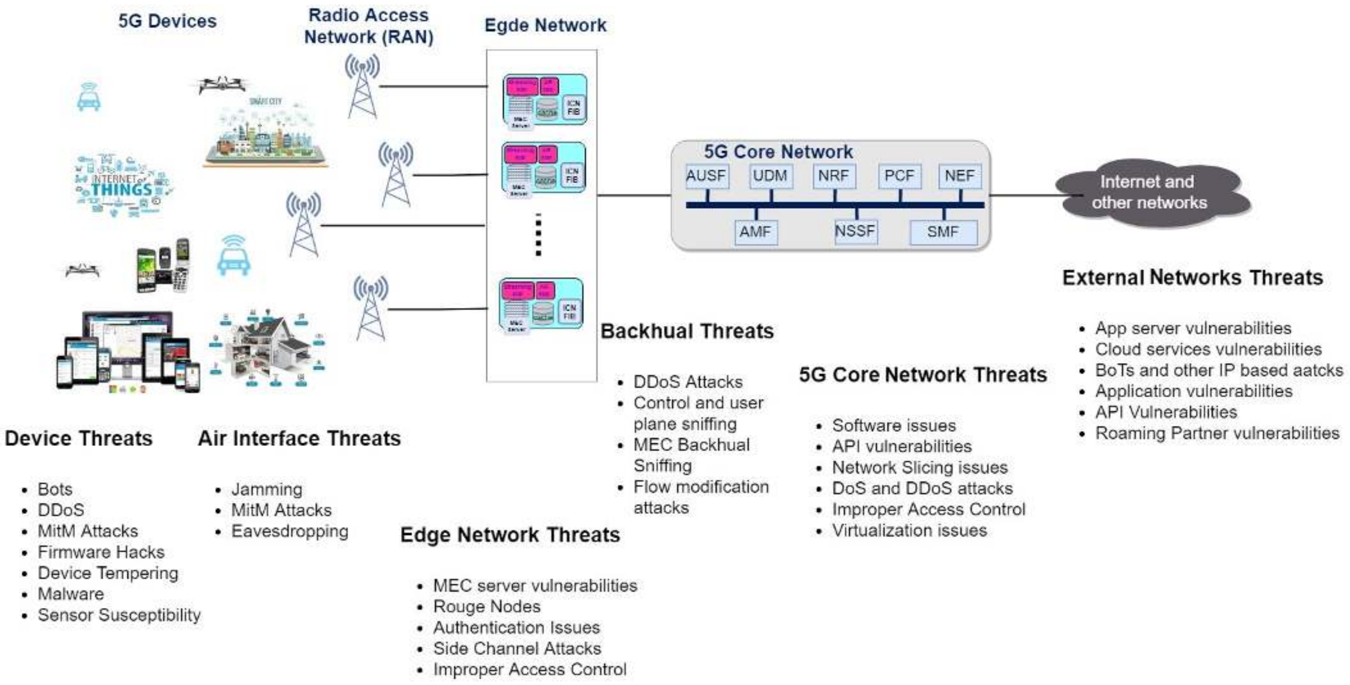


Fig. 13. Security Issues related to 5G Communication.

TABLE V
SECURITY ISSUES RELATED TO 5G COMMUNICATION

Attacked Segment	Security Attack	Description
User Equipment	Botnet	A botnet is a type of malware that can control a set of internet-connected devices. Mobile botnets can target many mobile end- in an automated way to perform different attacks (i.e. DoS, reply) on 5G systems. This threat is increasing as 5G will interconnect high power mobile phones [114]. Moreover, connectivity of IoT devices will open up new threat vector. Therese, IoT devices are vulnerable to IoT botnet attacks. E.g. In 2016, The Mirai botnet affected millions of IP cameras [115].
	Mobile Malware Attacks	Mobile malwares allow attackers to steal the stored personal data on the device or even launch attacks (e.g. DoS attacks) against other entities, such as other UE, the mobile access networks and the mobile operators core network [24].
Access Network	Attacks based on false buffer status reports	An attacker can exploit the buffer status reports of access network components such as BSs to obtain the information such as packet scheduling, load balancing and admission control algorithms, to achieve his malicious intents. Then attacker can send false buffer status reports by pretending as legitimate UE to jeopardize the operations [24], [25].
	Message Insertion Attack	Message Insertion Attacks are possible in 5G networks to initiate the DoS attacks. For instance, false flaw table updates can be used to overload SDN devices. In addition, An attacker can inject control protocol data units (C-PDU) to the system during the wake up time to preform DoS attack against the new arriving UE [21], [116].
	Micro cell Attacks	The physical size of BSs are drastically reducing and they be place in indoor locations such as malls, public places, stadiums and hospitals. Moreover, the use of new frequencies such as mmWave frequencies will also fuel the use of such micro BSs. However, these micro base stations are not physically secure as macro BSs used in pre-5G networks. Moreover, increment of number of BS will increase the potential vulnerability points in 5G Networks [117], [118]
Core Network	DDoS Attacks	DDoS attacks can be launched in a form of Signaling Amplification and HSS saturation by a using botnet to control a large number of infected UEs. [34].
	TLS/SSL Attacks	The TLS/SSL based communication used in SDN based Core network is vulnerable to attacks such as TCP SYN (Synchronization) DDoS, RC4 biases in TLS, Browser Exploit Against SSL/TLS (BEAST) attack, Compression Ratio Info-leak Made Easy (CRIME) attack, LUCKY 13 attack and POODLE attack [119].
	SDN Scanner	Attackers can passively collect network information such as IP of SDN controller and key network elements by analyzing SDN traffics. It is possible to perform various attacks such as DoS, TCP reset, replay and spoofing attacks by using the collected information [25], [119].

[139], authors proposed an IPSec based security architecture to secure the control channel communication.

In large-scale SDN networks such as mobile networks, multiple SDN controllers are used to control different network segments [140]. The SDN east/west-bound interface is used to establish Inter-Controller Communication (ICC) between

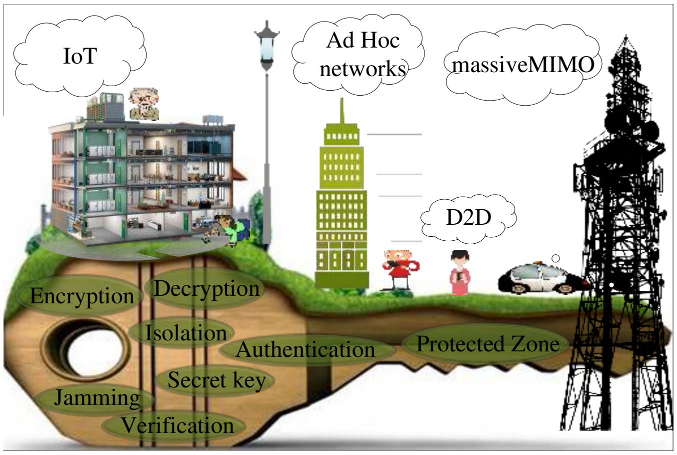


Fig. 14. Security Requirements for Access Control Network.

these multiple SDN controllers. This helps in sharing control information to perform various network functions such as security policy synchronization, mobility management, traffic management and network monitoring.

Thus, the security of these ICC channels is indispensable in ensuring the proper operation of the above functions. If the core ICC channel is compromised, then the whole system will be compromised regardless of what happens in the rest of the network. ICC channels of current SDN systems are vulnerable to a wide range of IP and web-based attacks such as DDoS, replay, IP port scans and Domain Name Server (DNS) hijacking [141], [142]. In addition, 5G ICC channels are also vulnerable to other physical threats such as technical failures, human errors as well as disaster failures. Inevitably, 5G ICC will be also vulnerable to a wide range of cyber and physical threats. Moreover, the existing SDN based communication systems have considered only the impact of cyber-attacks. For instance, Lam *et. al.* proposed to used Identity-Based Cryptography (IBC) protocol based secure key exchange mechanism to enhance the security of the east/west-bound data transmission in a multi-controller SDN networks [142]. However, this proposal did not address many known cyber-attacks and the physical threats.

While the industrial state of the art in 5G security advances in a reactive manner, current research in adaptive security offers a more flexible and resilient approach. However, security solutions in the current 4G networks are designed by different vendors; most are vendor proprietary solutions. Therefore, the mix and match use and real-time synchronization of different security solutions are extremely difficult or impossible in todays networks [143]. Thus, it is not possible to modify the existing system in real-time to prevent the ongoing attacks and new flexible security systems are required for 5G networks.

Moreover, security at the physical layer is an important area in 5G communications. A state of the art analysis of physical layer security is presented in the Section V.

D. Encryption

Encryption is particularly important to ensure the confidentiality of data. Due to the rich set of new network services, E2E encryption is significant in 5G domain. This can be used in different segments of the network to prevent the unauthorized access to the mobile data.

The radio traffic is encrypted in 5G at the Packet Data Convergence Protocol (PDCP) layer [82]. Similar to that of 4G LTE network, three different 128-bit encryption keys are used for user plane, Non-Access Stratum (NAS) and Access Stratum (AS). Moreover, the some of the 4G encryption algorithms will use in 5G New Radio (NR). As per 3GPP 5G standards [144], the same null, SNOW3G and Advanced Encryption Standard (AES) based EPS Encryption Algorithms (EEA) algorithms will be used in used in 5G as well. However, the identifiers are has been changed in 5G. 4G EEA (EPS Encryption Algorithm) is redefined as NEA (NR Encryption Algorithm) in 5G [145].

Ultra-Reliable Low Latency Communication (URLLC) is one of the major traffic class in 5G. In the RAN 5G NR achieves high resilience against security threats and attacks by deploying a single BS as two split units, called a central unit and a distributed unit [82]. This split helps to customizable deployment of security sensitive functions of the 5G NR access. For instance, user plane encryption is implemented at a secure central location and non-security sensitive functions are implemented in less secure distributed locations.

Moreover, encryption plays a vital role in privacy protection in 5G. To comply the latest privacy directives such as General Data Protection Regulation (GDPR) [146], [147] and the ongoing review of ePrivacy Directive [148], [149] in Europe, it is required to be considering the protection of privacy is a high priority requirement in the 5G systems. As a result, the subscriber privacy protection is included by design in 5G systems. In 5G subscriber identifiers, both long-term and temporary are protected by using a concealment mechanism which is based on the Elliptic Curve Integrated Encryption Scheme (ECIES) [150] and uses the home operator's public key [151].

In addition, ESTI technical committee on cybersecurity recently released two encryption specifications for Attribute-Based Encryption (ABE) which can be used in 5G and IoT. This is an asymmetric, multi-party cryptographic scheme that bundles access control with data encryption. The first specification was focusing on the personal data protection on IoT devices, cloud and mobile services when the secure access to data has to be given to multiple parties. The second specification focuses on the trust models, functions and protocols to control access to data in 5G networks [152], [153].

Moreover, the IMSI encryption [154] can be used in 5G to eliminating the threats of IMSI catchers [155]. IMSI catchers eavesdrop and track the subscribers. It violates the their privacy [155]. In [154], authors propose a new IMSI encryption algorithm to achieve this goal. A mobile device needs to generate a fresh pair of its own public/private asymmetric keys and random number. This is possible in 5G as the current USIMs are now capable of performing randomized asymmetric encryption operations [100], [156].

IV. Security Issues Related to Key Technologies in 5G

This section contains some of the most challenging security issues related to the key 5G technologies, i.e. SDN/SDMN, NFV, MEC, cloud computing and network slicing. Furthermore, the impact of these technologies on 5G security is also discussed in this section.

A. Security Challenges Related to SDN/SDMN

SDN arose as an attempt to present network novelties quickly, and to drastically streamline and automate the management of huge networks. Logically, the centralized control plane monitors and controls the whole system in SDN for packet forwarding inside the network [157]. Among several other technologies, SDN is one of the future 5G technologies that provides high reliability and high speed for the surge in network data and nodes for the upcoming years [158] [159].

Using two threat models, authors of [160] provided a comparative analysis between traditional and SDN network. The proposed model emphasizes a vital network assets required by the conventional production networks. For the coexistence of heritage and SDN-enabled networks, authors of [51] used three synchronization strategies for designing a data model. The proposed model stores the information for keeping Network Management System and controller synchronized.

Authors of [161] have proposed an security architecture based on big data analysis of secure cluster management for cluster maximized the control plane. It also includes an authentication technique for managing the cluster and an approach to optimize the control plane.

Authors of [162] have addressed the security vulnerabilities in 5G SDMN, network function virtualization and cloud computing by presenting a multi-tier component based security architecture. For raising SDMN security in control and data planes, the proposed technique contains five components including policy-based communication, secure communication, event management, security information and security defined monitoring. A robust security architecture for SDN-Based 5G networks was proposed in [138]. Here, the illegal requests from malicious attackers are identified by adding extra cryptographic authentication, termed synchronize secret. Thus, this scheme uses preload secrets to separate the attacks from regular network requests. Finally, Table VI summarizes the security issues related to SDN/SDMN and their relevance to pre-5G and 5G networks.

B. Network Function Virtualization Related Security Issues

The prior-5G mobile networks have network functionalities which are purely based on specific hardware and software.One physical node in the network plays a specific role. This will hinder the deployment and expansion on telecommunication networks in various ways. First, prior-5G mobile operators had to maintain a complex carrier network with a large variety of proprietary nodes and hardware appliances. Deploying new network services were difficult and costly. Also, it also took a long time to implement them. Adding a new service basically means that the network requires just another hardware. This needs to be integrated in the network. Due the rapid development of mobile network technologies, these services are quickly reaching to end of life. Therefore, these network services are needed upgrade quite frequently. However, this operation is quite expensive in current mobile networks due to existing procure-design, integrate-deploy cycle. Moreover, large and increasing variety of proprietary hardware appliances in operators network make it so complex and expensive to manage [179].

Thus, network operators were looking for a new means to make the network more flexible and simple by minimizing dependence on hardware constraints. NFV is a novel concept which refine the network equipment architecture. NFV virtualizes network services which were traditionally run on proprietary and dedicated hardware. Now, they can store in a cloud as a software application. The network is built by using commodity hardware and required network function can be dynamically deployed on such hardware according to the requirement.

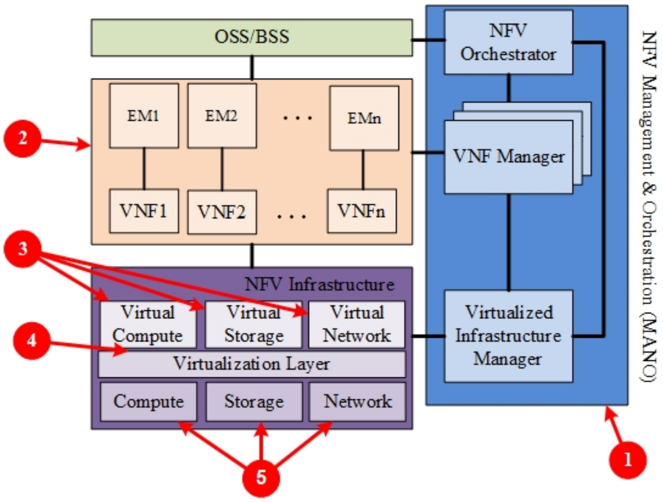


Fig. 15. Threat Vectors in NFV Architecture.

NFV can deliver several benefits. It reduces equipment costs (CAPEX) by removing under utilized equipment and eliminating the necessity to use proprietary hardware devices. NFV can significantly speed up the time to the market of new network services by reducing innovation life cycle of network operators. Furthermore, NFV enables the availability of network appliance multi-version and multi-tenancy. This allows a single hardware platform to share between different applications, services and tenants. NFV is also encouraging innovation to bring new services and generate new revenue streams. Thus, NFV will play a vital role in 5G network and one of the fundamental technology in 5G networks.

However, several security concerns found in 5G NFV systems. These security issues are mainly impacting on the resiliency as well as the overall quality of service in 5G networks. These attacks are ranging from physical hardware level to NFV architecture level. Specially, security attacks on software level components such as virtual infrastructure manager (VIM) got compromised other vulnerabilities can also arise exponentially [35]. Fig. 15 present the threat vectors

TABLE VI
SECURITY ISSUES RELATED TO SDN/SDMN

Threat Vector	Security Attack	Relevance to pre-5G	Relevance to 5G
Data Channel	Forged or faked traffic flows	Yes	Yes
	Eavesdropping	Yes	Yes
	Flow modification	No	Yes
	MitM (Man-in-the-Middle) attacks	No	Yes
	Replay Attacks	No	Yes
Switches	Clone or deviate network traffic	No	Yes
	Forged requests to overload the controller or neighboring switches	No	Yes
	Overload TCAM (Ternary Content-Addressable Memory)	No	Yes
	Fake controller based attacks	No	Yes
	Manipulating switch software	Yes	Yes
Control Channel	TCP level attacks	Yes	Yes
	TLS/SSL attacks	No	Yes
	SDN scanner attacks	No	Yes
	Lack of authentication	No	Yes
	Message modification attacks	Yes	Yes
Controller	DoS attacks	No	Yes
	Fake switches	No	Yes
	Software Vulnerabilities	No	Yes
	Backdoor Entries	No	Yes
	Attacks of East-West Channels	No	Yes
	Attacks via apps	No	Yes
Application Plane	lack of mechanisms to ensure trust between the controller and management apps	No	Yes
	Buggy software	No	Yes
	Unauthorized access via apps	No	Yes
	Insecure storage of apps	No	Yes
Admin Stations	Eavesdropping	Yes	Yes
	Buggy software	Yes	Yes
	DoS attacks	Yes	Yes
	Replay attacks	Yes	Yes
	Back door entrance	Yes	Yes
	Message modification attacks	Yes	Yes
	Software/OS vulnerabilities	Yes	Yes
Network Management	Lack of trusted resources for forensics and remediation	Yes	Yes
	Monitoring issues	Yes	Yes
	Virtualization related issues	No	Yes

related to NFV and Table VII summarizes the attacks related to threat vectors.

Comprehensive surveys of security issues related to NFV can be found in [35], [164], [180]–[182]. In addition, security issues in VNFs is presented in [170]. Security considerations for NFV cloud-based mobile virtual network operators are discussed in [183]. In [177], authors propose a new security mechanism based on Intel Software Guard Extensions (Intel SGX) to securely isolate the states of NFV applications to prevent the security vulnerabilities of stealing and manipulating the internal states of NFV applications that share same physical resources. Proposals for extending the current NFV orchestrator to have the capability of managing security mechanisms related 5G networks is proposed in [184]–[186]. In [187], authors define, review and evaluate Network Security Function Virtualization (NSFV) concept over Openflow infrastructure. NSFV has potential the security challenges related to network service provisioning, network monitoring and E2E security 5G networks. Security policy frameworks for NFV networks were proposed in [188], [189]. A security architecture for NFV-based communication networks is proposed in [190].

C. MEC and Cloud Related Security Issues

MEC is the network architecture that allows the cloud computing process usually on the edge of the network. In MEC, the functions required for the operation of the network occur near the UE and far from the network operator. Moreover, Edge devices are more vulnerable to physical attacks than cloud devices. In edge computing, the billing or changing data route occur through edge components only. Visited and home networks also depend on edge components. The core network can only keep a track of data received by the edge user to another UE via periodic polling [191].

Many authors provided solutions for some of the security challenges in MEC, cloud and combined MEC and Cloud networks. Fig. 16 depicts some of the relevant solutions of MEC and cloud computing networks. Zero-watermarking and visual cryptography are two proposed approaches to provide secure multimedia content and multi shared data. In [192], authors used above technique for providing biometric security solution for face images without affecting the pictorial worth of the image. Authors provide copyright protection to authenticate the multimedia content. In [193], authors have proposed a mobile edge computing framework for secure and shared user location in a crowded place using D2D communication with fog or edge nodes.

In [194], authors have proposed a distributed reputation management system to address the security issues in Vehicular Edge Computing (VEC). Authors of [195] have proposed a soft hesitant fuzzy rough set for appropriate security service

TABLE VII
SECURITY ISSUES RELATED TO NETWORK FUNCTION VIRTUALIZATION

	Attacked component	**Security Attack**	**Description**
1	NFV MANO (Management and Orchestration)	Malicious misconfiguration	An attacker get legitimate access to the orchestrator and manipulates the orchestrator configurations to change the operation of VNFs or grant access to run a modified Virtual Network Function (VNF) [163]
		SDN controller exploits	When NFV and SDN deployed together in 5G, the vulnerabilities related to SDN controllers or faulty controller can jeopardize the operation on NFV [164].
		DNS amplification attack	An attacker use public ally accessible open DNS servers to flood the orchestration with DNS response traffic [163], [165]
		Excessive log attack	Compromised VNFs can generate a large amount of logs which needed to be checked by VIM. If the compromised VNFs can generate enough number of fake logs, it can prevent VIM being checked the logs related to legitimate VNFs. In some cases, these fake logs can override the genuine logs [164]
		Log leak attack	Compromised VNFs can leak the infrastructure logs from one VNF operator to another operator to extract sensitive operational information [166]
		Privilege escalation	An attacker misuse the limited control dedicated to authenticated user to gain control over VIM to manipulate the management, resource provisioning and performance evaluation of operations of VMs [25]
		steal data form ephemeral storage	In a NFV environment such as OpenStack, attackers can steal data such as cryptographic keys from other VNFs ephemeral storage during Kernel-based Virtual Machine (KVM) live block migration since it does not properly creates all expected files [167]
2	VNF (Virtual Network Functions)	Inter-operability issues	Different VNFs are developed by different VNF providers and they have different level of security polices. The mismatch between these differences can lead to vulnerabilities when they are deployed in a same system. [168].
		DoS/DDoS	Many variety of DoS/DDoS attacks targeted services such as VNFs hosted in the Cloud, e.g attack on Bitbucket [169]. The impact of DDoS is even greater NFV since the attack could propagate to untargeted VNFs that are hosted on the same physical host [170], [171].
		Software flaws	Since VNFs are software, they are vulnerable to software flaws which can lead to unintended behaviours. For instance, these software flaws can be used to bypass firewall restrictions or do a buffer overflow to execute arbitrary code [170].
		VM escape attack	A malicious VM can escape out of the virtualization environment and execute arbitrary code within the hypervisor to compromised it [172].
		VNF Manipulation Attacks	An attacker misuse the privileges of compromised hypervisor to install kernel root kit in VNF's OS and manipulate the VNF [164].
		VNF location shift attack	An attacker can migrate an compromised VNF to a different location which has less security or privacy policies to gain addition access to the system [164]
3	VM (Virtual Machines)	VM Migration attacks	During the VM migration, MitM attacker can modify arbitrary VM OS or application states [173]
		Side-channel attacks	An attacker obtains the information in an indirect manner to attack the targeted VMs. For instance, attacker can measure the frequency of other VMs, that are are paused to predict the pause time of targeted VMs [174]
		Scheduler Attacks	An attacker use the vulnerabilities in the hypervisors scheduler to acquire system resources for the malicious VM at the expense of a victim VM [172]
		Lack of Isolation	Due to the lack of proper isolation between VMs, an attacker can utilize a compromised VM to communicate and propagate security threats to co-hosted VMs on the same physical host [175]
		VM Data theft	A malicious VM which is infected with malware can use the memory bus or cache contention to stealthily steal data, e.g. cryptographic keys from the co-resident VMs [176]
		VM rollback attack	An attacker uses an older snapshot of VM without the concern of VM owner to bypass the security system and obtain the access the system. This attack is possible after an already comprised hypervisor roll back to its the previous snapshot [176]
4	Hypervisor/virtualization layer	VM/guest OS (Operating System) manipulation	The guest OS vulnerabilities such as OS command injection, SQL injection, buffer overflow or missing authentication for critical function can be utilized to attack the hypervisor in the hosting OS [35]
		Isolation Failure Risk	Lack of proper isolation can be use to break into a hypervisor by compromising some VNFs running over it [164].
		Exhausting Hypervisor	some VNF applications can be manipulated to consume high CPU, hard disk, and memory resources so that, they can exhaust the hypervisor [164].
		Exceeding Logs Troubleshooting Failure	VNFs can be compromised to generate a huge amount of log entries on the hypervisor. Then, it will difficult to analyze logs from other VNFs, especially, when the initial entries in the log files are deleted.
		Insider attacks	When a malicious administrator has the root access to the hypervisor and by using a search operation. He can extract the user ID, passwords and SSH keys from the memory dump, which in turn violates user privacy and data confidentiality
5	Physical Hardware	Disk failure, Physical attack	A physical attack (i.e. power cutout, link break and fire) on hardware will terminate the availability of hardware resources for VMs [35]
		Code execution on the physical host	A compromise VM can execute on the host physical hardware to read/modify the stored data, deny the physical resources or disrupt the services for co-located VNFs [171]
		State Manipulation Attack	Attackers steal and manipulate the internal states of NFV applications that share a same physical resource [177]
		Resource Interference Attack: I/O	A malicious VM or VNF can also steal the scheduling characteristics of the hypervisor to overload I/O resources available for other co-located VMs or VNFs [171], [178]
		Resource Interference Attack: CPU	A malicious VM or VNF can over utilize the CPU resources of host hardware to deny the availability of processing resources for co-located VMs or VNFs [171], [178]

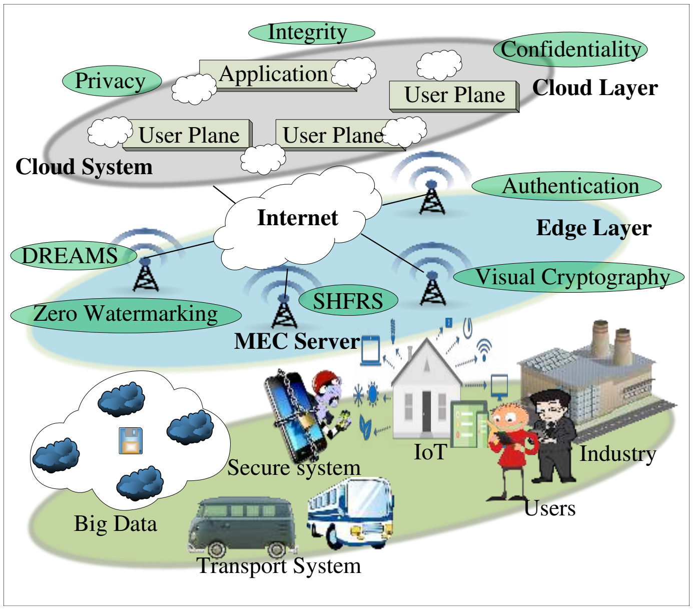


Fig. 16. Security Mechanisms for MEC and Cloud Network Systems.

selection in real-time multi-criteria decision making problems for Fog and Mobile-Edge Computing (FMEC). For enhancing the security trust for Mobile Social Networks (MSNs), authors of [196] have presented a social trust scheme for trust based MSNs with MEC. They resorted to the knowledge of social relationships for improving security and efficiency. For supporting IoT in MEC, authors of [197] have scrutinize to security issues in IoT applications of MEC.

In the new era of 5G technology, constant generation of enough data by several applications certainly needs a cloud based system. It is unwise to store the data in the end devices due to limitation of space, energy, reliability and vulnerability. Integration of mobile computing and cloud computing together extends the limitation of storage with Mobile Cloud Computing (MCC). Mobile users can save data at any time from anywhere. However, it faces a number of challenges in terms of privacy, data integrity and security. A number of authors provided certain security mechanism for respective scenarios that are suitable for the MCC system security.

Authors of [198], [199] proposed security protocols for MCC. In [198] authors designed a secured and efficient system for data distribution in MCC. The proposed system provides data authentication, privacy, integrity and flexible data distribution with access control without involving a third party. Considering the security issues in MCC, authors of [199] have proposed a chaotic fuzzy transformation method of allowing search process of user's secured encrypted data on the cloud. The proposed scheme guaranteed the confidentiality and privacy. Authors of [200] have proposed a light weighted data-sharing algorithm (LDSS-CP-ABE) for MCC.

With a suitable structure of access control technology Ciphertext-Policy ABE (CP-ABE), authors of [200], [201] have adopted it to offer cloud security in the systems. A proxy encryption and a ciphertext-policy ABE scheme have designed by the authors of [201] for P2P storage cloud. Authors have also proposed an efficient, fine-gained and ciphertext-policy for a secure P2P storage Cloud access control mechanism.

In [202], authors have designed a flexible, efficient and secure retrieval system based on fog and cloud computing. Authors of [203] have presented an algorithm for workflow applications on federated clouds by introducing an entropy-based method of quantifing the most reliable workflow deployment and fulfill security requirements by extending the Bell-LaPadula Multi-Level security model. Authors of [204] proposed a deterrent-based scheme to secure the knowledge of data exchange between various data owners from a dishonest cloud server. Authors of [205] proposed a secure data self-destructing scheme that serves as a Key-Policy ABE with Time-Specified Attributes (KP-TSABE) for cloud computing. The proposed scheme supports the time interval labelled ciphertext with time instant associated private key. Authors of [206] proposed Smart-Frame that provides a secure cloud computing based framework for information management of big data on smart grids.

D. Network Slicing related Security Issues

Recently the rule of divide and conquer has been chosen for 5G. Thus, Network Slicing (NS) concept is the integral part of 5G. It is a specific form of network virtualization techniques to deploy multiple logical/virtual networks to run on top of a single shared physical network infrastructure. The main purpose of using network slicing is partition the physical network resources to optimally group the different traffic, isolate from other tenants and configure the network resources at a macro level [207].

Each slice is separated in terms of a case/field with the specific required operations. The logical slicing divides a single common physical network into various virtual, complete E2E networks. It provides complete isolation for these virtual networks from each other in terms of access, transport, device and core network. These slices are dedicated to different types of services and scenarios. The target during division is to customize and optimize each network in terms of resources, QoS, and security. Therefore, NS is utilized in E2E manner which consists not just networking resources but also computing and storage resources.

The key benefit of NS is that, it allows MNOs to partition their network and network resources to accommodate very different users and different traffic classes. For instance, NS can be used to simultaneously accommodate different 5G traffic classes i.e massive Machine Type Communication (mMTC), enhanced Mobile Broadband (eMBB), and Ultra Reliable Low Latency Communication (URLLC) on a same physical network infrastructure. These traffic classes have very different characteristics. For instance, mMTC is related to providing the connectivity for a very large number of IoT devices, which may have very low throughput. However, eMBB has the opposite properties as this traffic class is focusing on transporting very high bandwidth content and services.

The concept of network slicing is somehow similar to VPNs (Virtual Private Network). However, 5G calls for new methods of slicing as it has a wider scope and requires implement in most challenging environments. Network slicing can be considered as on-demand networks. They can be deployed, eliminate and removed from any network dramatically. Network slicing is can be used in RAN as well. Here, a unit physical network is divided into several virtual networks that can support various RANs. It is envisaged that network slicing will play a major role in 5G as it can improve the flexibility, operation of the infrastructure and the distribution of resources.

Security of NS is an important factor for successful deployment of network slicing [207]. For instance, a controlling mechanism is required for the inter-network slices communication including the management plane communication, signaling, undesired communication between functioning and network operator. For the communication between functions, slices and interfaces between them, a proper mechanism is required to ensure a secure operation within expected parameters along with operators security requirements. If the communication channel between different slices is not secure, attackers can disrupt the communication between slices. This will leads to resources under utilization as life cycle management of slices will not happen properly [208].

Within an operator network, neither a host (physical) nor a network slice manager can be considered as impersonal if the network slice manager dynamically create or destroy a network slice and map and load them to accessible the physical host platform. For a safe and secure transmission, both network slice manager and the physical host must recognize each other through authentication. Similarly, in the case with more network slice managers within an operator network; all network slice managers must authenticate each other [209].

Particularly it is difficult protect the virtual elements that run within the slice have destroyed, moved or replaced with another newly created instance. It might have done by a malicious or non-malicious actor. An impersonation attack against a network slice instance impact on all of its services. Therefore, authentication is required for network slice instance as well [144], [208].

Each slice has different protocols and network services with different security level due to the requirement or the assigned task, it needs to perform or may be due to different latency requirements. However, this must not affect the security level of another slice. Recommendation is to design a baseline security level collectively for all the layers without any excuse. For the unavailability of baseline scheme, all layer security must be equally good and protectable. In addition, when UEs are capable of accessing all network slices separately then either they should authenticate themselves before accessing each slice or they need to first access the low security slice by authentication then access high security slice [208], [210].

DoS attack is possible for exhausted resources. Exhaustion of common resources for all slices provides high probability of attack on other slices too. Provision of capping resources and optionally ring-fencing resources assure maximum and minimum recommended levels of resources. Ring-fencing network resources provide ability to run resources for security protocol even in case of exhaustion [208].

Another attack is the side channel attack, which results in the leakage of any cryptographic information. Particularly, when two slices share some primary hardware. In case of any cryptographic information leakage, the security of the sharing hardware device may compromise. It can be prevented with the strong isolation of virtual machines that prevents the code exposure of one machine due to the code exposure of another machine. Moreover, in case of different slice sensitivity level, it is better to avoid co-hosting on the same hardware slices [144]. In hybrid deployment models where the operator deploys the combination of virtual and regular functions. Such deployments must keep at least regular security level. Utilization of multiple services by the user with different slices at the same time requires a proper sealing between slices. Proper investigation will provide a better solution in this context. The offered security mechanism should exist not only in the UE but also in the network for better protection [208]. Table VIII summarizes the key security issues in network slicing related to 5G.

TABLE VIII
SECURITY THREATS RELATED TO NETWORK SLICING

Threats	Description
Attacks on inter-network slices communication	An attackers can disrupt the communication between slices to prevent the proper life cycle management of slices.
Impersonation attack	An attacker can impersonate as an physical host platform to allocate unavailable resources. Moreover, an attacker can impersonate as network slice manager to steal network slice creation parameter
Security policy mismatch	Variance of security policies and security protocols for different slices allow attackers to access the NS system and control entities via less secure slice.
DoS attack	An attacker perform an DoS attack either on vitalization platform or physical resources to exhaust the available network resources for other slices
Side channel attacks	An attacker gain access to one slice and attack the a set of slice which share the same primary hardware.
Privacy attacks	Infrastructure providers or VNF suppliers steal the cross slice user information.
Hypervisor attacks	Perform attacks against the hypervisor to jeopardize the virtualization of resources. These attacks includes, software erros in hypervisor, backdoor entry via hosting OS, DoS attacks and attacking the hardware resources

V. PHY SECURITY

PLS in offering safety measures for data secrecy. It has received a noteworthy research interest. The growth towards 5G wireless communication positions new challenges in physical layer security community. This target can be achieved, by using advanced channel codes or by resorting to introducing key generation. There are two main candidate channel codes are identified by 3GPP community [230] namely, Polor codes [231] and LDPC codes [232]. The main technical challenges which continue to be unsettled at a substantial level while there are many ad-hoc solutions are presented in the literature in relation 5G networks. This section highlights the potential PHY layer security challenges and current presented solutions in other key 5G technologies such as OFDMA, NOMA, UAV, mmWave, massive MIMO, channel coding, energy harvesting and some other related issues. Fig. 17 and Table IX give a brief overview of this section.

TABLE IX
PHYSICAL LAYER SECURITY A BRIEF REVIEW

Ref	Key Technologies	Considered Scenario	Goal and achievements
[211]	OFDM-SC, PLS, URLLC, FDD, TDD	Single cell SISO OFDM for DL OFDMA, Rayleigh multi-path fading, direct communication with QPSK modulation and knowledge of CSI and security techniques for eavesdroppers.	Secrecy and reliability through OFDM-SIS algorithm based on URLLC.
[212]	PLS, AN, Jamming position selection, polar codes and Bhattacharyya parameters	A DL communication system with fixed fading coefficients, no spatial freedom and no additional power.	Improvement of secrecy rate with AN aided polar coding and sub optimal jamming position selection using greedy algorithm and channel polarization. Authors have also used cryptography.
[213]	A number of eavesdropper and relay, DF network, single antenna relays, Multi-hop massive cooperative relaying	Single cell ad-hoc HD communication system with multiple relay cooperation, cooperation among eavesdroppers with MRC of wiretapped signal and independent eavesdroppers with and without MRC.	Better PLS of 5G large scale relay networks. Authors proposed GD-CAES, MM-CAES, and DA-CAES using graph theory.
[120]	Stochastic geometry, access selection, optimization	Single Cell DL communication system with small and large scale Rayleigh fading.	Maximized secrecy throughput with proposed search algorithm using stochastic geometry.
[214]	Stochastic Geometry	A Single cell and multiple antenna on BS for UL NOMA with quasi-static Rayleigh fading, unknown CSI, imperfect SIC, and passive eavesdropping.	Effective secrecy throughput with stochastic geometry.
[215]	NOMA with cooperative relaying and beamforming	A Single cell SISO DL NOMA cooperative communication system. Relay is considered to be far from BS and near eavesdropper.	Maximized secrecy rate region of LUs with cooperative communication.
[216]	Alternative search method (ASM), successive convex approximation, monotonic optimization	HetNet, DL, PD-NOMA with Rayleigh fading, multiple eavesdroppers.	Optimized sum secrecy rate based on optimization.
[217]	Stochastic geometry	Single cell, DL NOMA with Rayleigh fading channel, randomly deployed users and eavesdroppers.	Secrecy for NOMA using stochastic geometry.
[218]	Stochastic geometry, single antenna, multiple antenna	Single cell, DL NOMA with Rayleigh fading, randomly deployed users and eavesdroppers.	Secrecy in NOMA for single and multiple antennas using stochastic geometry.
[219]	PS-NOMA, optimization	Single cell, DL, OFDMA with Rayleigh fading.	Secrecy in PD NOMA via proposed iterative algorithm and optimization.
[220]	OFDMA	Single cell, DL, OFDMA with Rayleigh fading.	Resource allocation for maximized fairness for the user's secrecy rate with the proposed three low polynomial complexity heuristic algorithms and optimization.
[221]	Massive MIMO	Single cell MIMO, DL, TDD, block fading, training phase and no training phase jamming.	Secrecy in MIMO with the proposed $\delta-$conjugate beamforming in mMIMO.
[222]	ZFBF, MIMO HetNet	Macro and pico cells, DL, TDD, Rayleigh fading and MIMO is combined with HetNet.	Improved secrecy with MIMO HetNet based on mMIMO HetNet systems.
[223]	OFDMA and CRNs	single cell	Trade-off between secrecy and robustness with the proposed iterative algorithm and optimization.
[224]	OFDMA and CN	Single cell with a primary and secondary links, DL, OFDMA with Rayleigh fading in a cooperative scenario.	Average throughput for open and private information via proposed cross layer scheduling and spectrum access.
[225]	SWIPT	Single cell, DL, OFDMA, Rayleigh fading with open and private information to multiple users.	Secrecy and optimum harvest power with the propsed iterative and two-step algorithm.
[78]	WSNs, cooperative jamming and AF	A single cell, DL OFDMA cooperative scenario with small scale fading and CJ.	Secure network with proposed near optimal resource allocation algorithm.
[226]	OFDMA	Single cell UL OFDMA system with Rayleigh fading, DF and known CSI.	Secure resource allocation with optimization approach.
[227]	OFDMA	Single cell DL, OFDMA flat fading direct communication with perfect CSI.	Secrecy rate or fairness using jamming power.
[228]	OFDMA	Single cell, DL, OFDMA, large and small scale fading with known CSI.	Secrecy.
[229]	OFDMA and CRNs	single cell with primary and secondary BS, DL, OFDMA, Rayleigh fading cooperative scenario with unknown CSI.	Secure communication in CRNs with optimization.

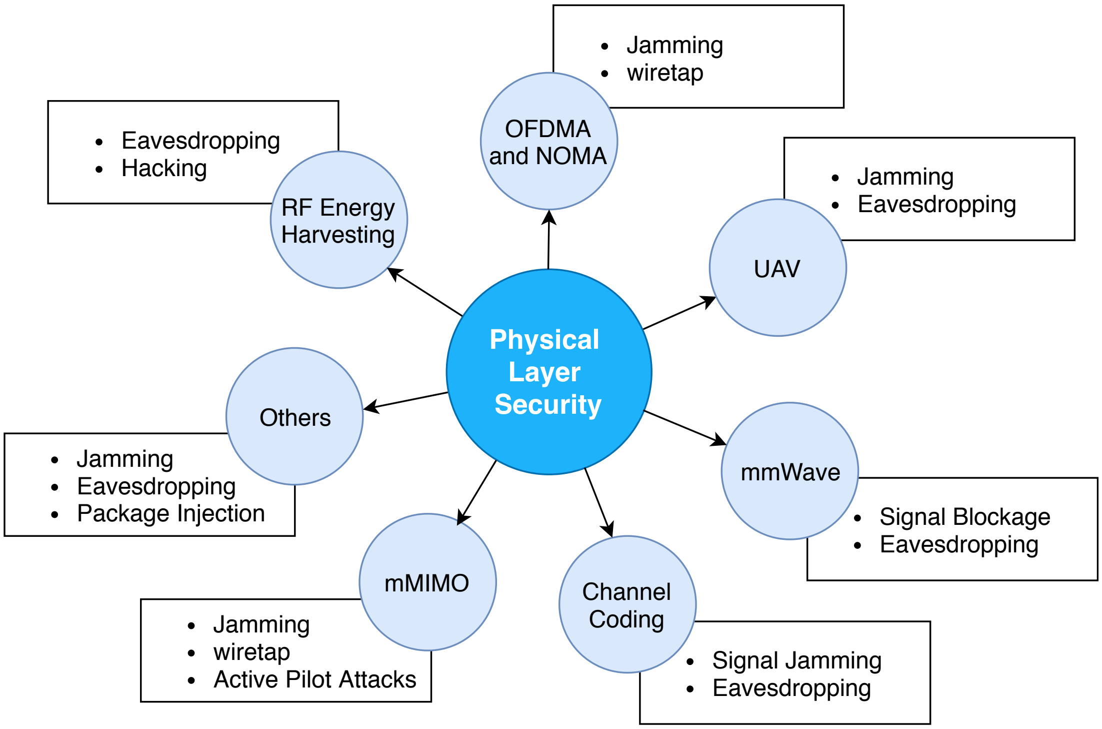


Fig. 17. 5G Network Security in Physical Layer.

A. *OFDMA and Non Orthogonal Multiple Access (NOMA)*

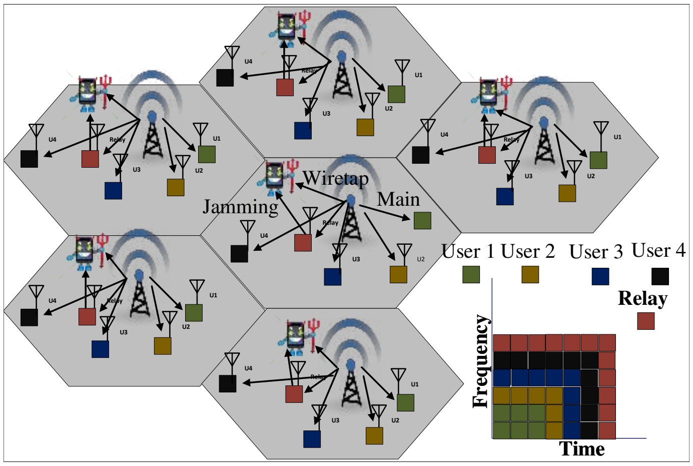


Fig. 18. Security challenges and solutions for OFDMA PLS. When BS observes the outside world then take decision and then act accordingly. In such case, OFDMA is combined with CRNs.

OFDMA is superior among all the medium access technologies. This improves the spectrum efficiency largely and fulfills the requirement of 5G technology. There exist several other benefits of using OFDMA including Inter Carrier Interchange (ICI) and the Inter Symbol Interchange (ISI) problems. It is one of the latest and on-demand technology. However, it faces few security challenges in its implementation. This section contains the identified key problems and the solutions related to the security of OFDMA. However, it still offers an open research area for the scholars and scientists. Fig. 18 shown the basic infrastructure with certain security issues in OFDMA.

Researchers often utilized joint power and resource allocation techniques to provide better secrecy in the network . In [220], authors intended to provide a solution for assigning sub-channels and power in a multi-user DL OFDMA system to boost the max-min fairness standard over the users secrecy rate. In [227], authors proposed to utilized jammer's power in a DL OFDMA system for improving secrecy rate or fairness. It has proved by the authors that the maximum jammers power offers the maximum secrecy rate. Authors of [225], studied the power splitting ratio selection and joint sub-carrier allocation for secure DL OFDMA-based SWIPT networks.

Cooperative jamming or jamming techniques are also helpful to provide high secrecy rate. The authors of [78], investigated joint sub-carrier allocation, sub-carrier pairing and power allocation for a secure two-way relay in OFDMA WSNs with and without CJ. Without CJ, the authors proposed near optimal resource allocation algorithm which appropriately allocates resources with the improved secrecy sum rate. With the CJ keeping the Relay Station (RS) up-to-date, eavesdroppers are kept confused. For a secure OFDMA Decode and Forward (DF) networks, authors have proposed a scheme for limited rate feedback resource allocation.

In [228], authors have proposed AN generation and removal methods for OFDMA based SWIPT. Jointly optimization of transmitting power and SC allocation for AN signals helped in maximizing the sum secrecy rate for Information Receivers (IRs) that are subjected to constraints of individual harvested power of Energy Receivers (ERs).

Based on OFDMA, Cognitive Radio Networks (CRNs) also provide network security better than other techniques. In [223], authors have proposed several strategies for providing trade-off between robustness and secrecy of the system in a secure ergodic resource allocation (SERA) problems in relay assisted OFDMA based underlay CRNs with passive eavesdroppers. This is called Secure Robust Ergodic Resource Allocation (SRERA) and in [229], authors have proposed two cooperative communication schemes with MRC and without MRC in a OFDMA based CRNs for a secure system of communication. In a OFDMA based CR network, the author of [224] has proposed an algorithm for cross-layer scheduling and spectrum access to optimize the average throughput of private and open information.

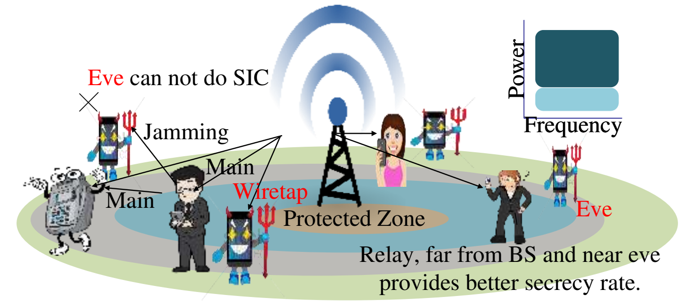


Fig. 19. Security challenges and solutions for NOMA PLS. When BS observes the outside world then take decision and then act accordingly. In such case, NOMA is combined with CRNs.

Another innovative efficient technology NOMA, recognized as one of the candidates of 5G technology. NOMA provides several advantages; high spectrum utilization, fairness, QoS, robustness, data rate, and throughput over other existing technologies [233]. M-NOMA [234], [235] is a modulation based energy efficient technique which provides better system complexity, interference, data rate and SER. Due to the least spectrum division, it is certainly vulnerable to a number of security threats. Therefore, before the implementation of NOMA in the real world, a number of authors provided suitable way to tackle the upcoming probable security issues. Fig. 19 shows security challenges and solutions for NOMA PLS.

For the secrecy of NOMA, a number of authors were focusing on providing secure regions to the legitimate users (LUs) for better security. In [214], authors have provided a protected zone around the LUs or established an eavesdropper's exclusion region. In [215], a perfect cooperative scheme is presented that depends on the number of relays and their distances from the BS and eavesdroppers. The target is to optimize the secrecy rate region of the LUs subject to the power constraints on the relays transmission and the BS. As of [217], to enhance the secrecy performance in NOMA large scale networks, expanding the choice of the protected regions or reducing the choice of the user regions is required. Additionally according to [218] by generating AN, BS communicates with randomly distributed NOMA users via single or multiple antennas.

In [216], authors proposed a scheme which prevents an eavesdropper from performing Successive Interference Cancellation (SIC) (even if they know the channel ordering). Moreover, authors formulated an optimization problem of joint sub-carrier and power allocation to increase secrecy rate in DL PD-NOMA HetNet with multiple eavesdroppers.

In [219], authors studied the optimal design of allocated power, decoding order, and transmission rate for maintaining secrecy in PD-NOMA. In the considered scenario, channels of the eavesdropper with passive eavesdropping are unknown. In [236], authors discussed the PLS is combined with NOMA and CR networks . The wiretap network modelled for the technical requirement of combined CR NOMA. In [237], authors have offered a Chaos NOMA (C-NOMA) for secure multiple access transmission. They offered another C-MIMO scheme as a channel coded communication scheme using communication principle of chaos. In [238], authors have proposed a low complexity Sub-Carrier Assignment Scheme (SCAS-1) in a NOMA using amplify-and-forward two way relay wireless networks. The proposed scheme jointly assigns secure sub-carrier and power to the system of NOMA.

B. UAV Assisted Security

UAVs have been widely used for a variety of applications including civilian and military purposes. The research on UAVs has increased by U.S military investment since 2012 largely. It includes armed attacks, surveillance, reconnaissance and transportation. UAVs are autonomous, automated, reliable and remote devices. Due to the ability of data storage, UAVs may store secret information or any type of useful data depending on the type of application of UAVs. Therefore, they are highly vulnerable to several attacks. For the purpose of their security, it is required to investigate suitable security measures. Recently, UAVs security became one of the major research concern due to the amount of information they carry in the airborne. Due to air-to-ground Line Of Sight (LOS) transmission, it brings a great challenge for network security. Fig. 20 shows the security challenges with some of the related solutions for UAV PLS.

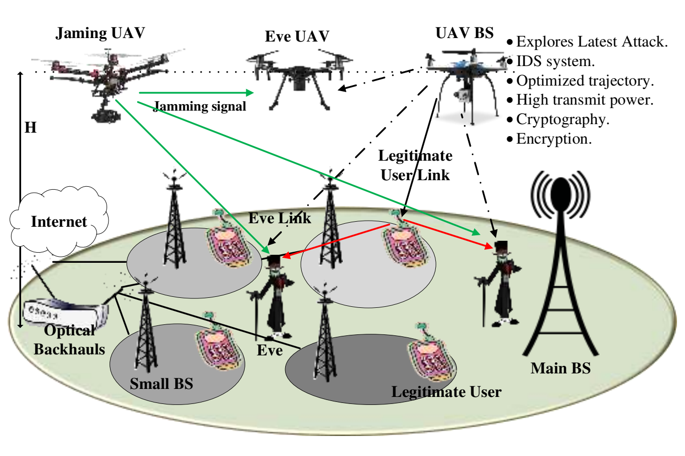


Fig. 20. Security challenges, detection and solutions for UAV PLS.

Several key UAV security techniques were proposed, which were depending on Intrusion Detection System (IDS) and response mechanism. In [239], authors have explored the latest attacks and developed a system for threat assessment of UAVs centered on the condition of services and communication infrastructures. The authors considered the communication system, sensor systems, fault handling mechanism, storage media and other exposed factors. For the security analysis, authors have used AR Drone, MQ-9Reaper, and RQ-170 Sentinel. In [240], authors have proposed an IDS based on the adaptive specification. IDS detects any malicious attack on UAVs for the importance of continuous operation of an airborne system. On the other hand authors in [241], have proposed a hierarchical intrusion detection and response scheme. The proposed scheme works not only at the ground level stations, but at the UAVs as well. The detection scheme also used to characterize the type of attack. The proposed scheme targets specially the lethal cyber-attacks like GPS spoofing, false information dissemination, black hole, gray hole and jamming attacks.

In [242], authors proposed PASER for low-altitude UAVs combined with WLAN mesh networks (WMNs). PASER fulfills the security requirement of a UAV-WMN. The proposed protocol detects more attacks than IEEE 802.11s/i and Authenticated Routing for Ad hoc Networks (ARAN). In [241], [243], have addressed two main issues in the context of attacker ejection and intrusion detection; attacker ejection and activation of the intrusion monitoring process.

The optimization of secrecy rate is one of the active research areas. Many authors proposed various technologies to achieve maximized the security rate. For transmitting confidential information from UAV to multiple ground users, authors in [244] proposed an iterative algorithm to facilitate the optimization problem. In [245], authors have proposed an iterative suboptimal algorithm to solve the problem of maximizing the average worst-case secrecy rate by mutually optimizing the trajectory and the transmit power of UAVs ground communication system with multiple imperfectly located eavesdroppers. Authors of [246] have discussed Secrecy Energy Efficiency Maximization (SEEM) problem for UAVs trajectory planning. An efficient iterative algorithm based on SCP and Dinkelbacks method is used to obtain the solution of the problem under discussion. In [247], authors formulated a Prospect Theory (PT)-based smart attack game to resist the smart attack for the UAV transmit power allocator on multiple radio channel. In the observed scenario, deprived of having the information of attack detection precision of UAV, an intruder chooses the kind of attack from eavesdropping, jamming and spoofing. Authors have proposed different power allocation strategies for tackling the unknown attack by the intruder.

To secure UAVs, many researchers provided different cryptographic scheme to authenticate the system. In [248], authors have proposed an enhanced Direct Anonymous Attestation (DAA) cryptographic scheme called Mutual Authentication DAA (MA-DAA) for Network Connected-UAV (NC-UAV) units without human intervention. The enhancement of cryptographic scheme DAA is required due to its capability of limited transmission bandwidth and low computing in UAV. The proposed scheme provides a low computational cost, high efficiency and improved mutual authentication. Considering no prior knowledge of the attacker, authors of [249], have proposed an generalized log-likely hood ratio (GLLR) based authentication scheme to encounter the spoofing attack of the control signal in a UAV system. In [250], author provided a biometric system of encryption between computerized BSs and UAVs using Electroencephalogram (EEG) beta component signal from users' device. A proper jamming of signals for eavesdroppers also guarantees the security of the network. In [251], authors have proposed caching assisted UAV for secure transmission in hyper-dense networks. In the proposed study, Idle SBSs replaced by the UAVs which generates jamming signals for the eavesdropper to provide secure transmission. Authors in [244], dedicated some of the UAVs for signal jamming wiretap channels only. Authors of [252], analyzed 3D UAV-enable mmWave with the consideration of real-world constraints of UAV and exclusive features of air-to-ground channel. Authors used part of UAVs to transmit jamming signals to intruders for a better characterization of security.

C. mmWave

There are three promising technologies for 5G era communication including mmWave, massive MIMO and HetNet. These are some of the technologies among robust and efficient wireless transmission proposed techniques [53]. To fulfill the high capacity network requirements in 5G communication networks, high demand for spectrum is intended to accomplish by utilizing the mmWave band of the spectrum. The unlicensed gigahertz bandwidth of the spectrum bestows mmWave communication with great potential to offer optimum data rate due to expected abundance of bandwidth. Fig. 21 shows the security challenges in mmWave PLS with the range of mmWave spectrum.

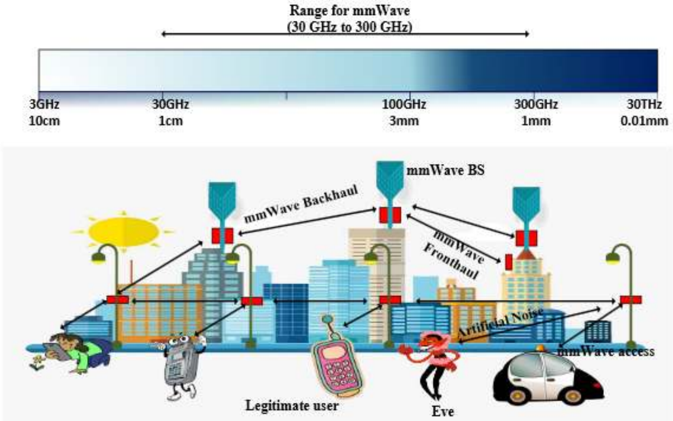


Fig. 21. Security challenges and communication of mmWave in PLS.

For mmWave security, most of the authors have combined mmWave with MIMO to provide secured transmission and included the behavior of AN to observe the network security performance. Authors of [253], targeted to provide high network security by designing secrecy beamforming MIMO AF two-way cooperative network through mmWave. For vehicular MIMO mmWave communication security, authors of [254], proposed two techniques of PLS. In the first technique, authors have used a single Radio Frequency (RF) chain for transmitting information signals to the intended receiver and noise resembling signals in the direction other than the receiver. In the second scheme for transmitting radio signal to the target receiver and inject AN in the controlled direction with a few RF chains.

To improve PLS in mmWave wireless communication system, authors of [255], have proposed hybrid MIMO phased-array time-modulated Directional Modulation (DM) scheme. Similarly, with partial channel knowledge in MISO mmWave systems authors of [256] proposed a hybrid analog-digital procoder design. In [257], authors have characterized the secrecy performance for AN aided and noise limited mmWave network. For mmWave networks, Authors concluded two significant parameters for the enhancement of system secrecy i.e.; eavesdroppers intensity and array pattern.

For PLS security in mmWave large-scale antenna systems, authors of [258], have designed hybrid precoders with two types of channel knowledge. Authors have proposed an iterative hybrid precoder design to exploit the secrecy rate and to minimize the secrecy outage probability. For multiple transmitting antennas, large-scale mmWave ad hoc networks, authors of [259] have proposed to assess an average achievable secrecy rate for the exceptional situation of Uniform Linear Array (ULA). Along with the proposed technique authors have characterized impact of mmWave channel characteristics, antenna gain, random blockages, and impact of AN in these networks. Authors of [259] concluded the requirements of low transmit power with low mmWave frequency and with high transmit power for better secrecy performance of the network.

Additionally in [260], the authors aimed to improve the system security by developing the mathematical framework to analyze the secrecy outage probability, connection outage probability, and achievable secrecy rate in hybrid mmWave-overlaid microwave cellular networks. A conventional fading model cannot precisely model the arbitrary fluctuations of mmWave signals. Therefore, the Fluctuating Two-Ray (FTR) fading model has proposed by the authors of [261] to provide PLS in mmWave communication system. Authors have derived the analytical expressions for the probability of strictly positive secrecy capacity, average secrecy capacity and the secrecy outage probability.

MIMO is a very useful technique in various applications of wireless communication, due to the flexibility, secure and better coverage. MIMO can be considered as an integrated combined technique with NOMA, OFDMA, mmWave and UAV in terms of security. A number of researchers obtained multiple solutions for MIMO network by using beamforming, AN, secrecy outage capacity, cooperative relay networks, channel estimation and others. Fig. 22 shows the general overview of the security challenges and solutions for massive MIMO.

D. Massive MIMO

Beamforming is one of the special characteristics in MIMO networks. Authors utilized it to provide better secrecy performance. In the beam domain of single-cell secure massive MIMO network, authors of [262] have developed an effective iterative and convergent algorithm for optimization of secrecy sum rate and power allocation with a multiple antenna passive eavesdropper. With known statistical Channel State Information (CSI) at the BS, authors of [262] introduced a lower bound on the achievable ergodic secrecy sum rate and derived the condition for eigenvectors of the optimal input covariance matrices to maximize the lower bound secrecy sum rate.

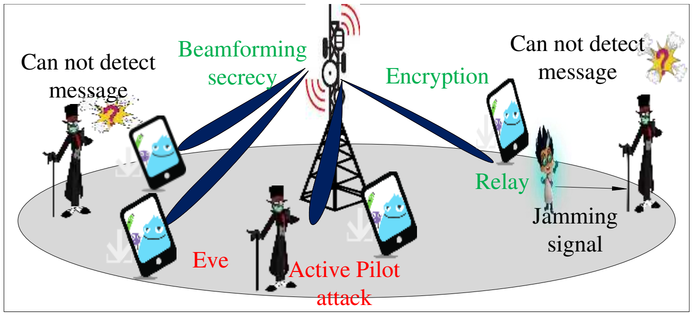


Fig. 22. Security challenges and solutions for massive MIMO PLS.

In [221], [263], authors studied the secure TDD massive MIMO for physical layer and showed that the massive MIMO communication is logically resilient towards no training-phase jamming attacks. Authors of [221] have proposed a δ-conjugate beamforming for establishing an information theoretic security for a certain number of antennas. Authors also observed the system under training phase jamming showed zero maximum secure Degrees of freedom (DoF) attained and emphasized the importance of cryptography.

Usually, the purpose of AN is to confuse eavesdroppers in a system. Improvement of secrecy capacity is a main concern with AN schemes. In most of the AN schemes, a number of transmitting antennas are assumed to be higher than receiving antennas to utilize all eigen-subchannels in a MIMO system. In [264], authors have proposed an AN scheme to improve secrecy capacity in a MIMO system. In the proposed scheme, authors used strongest eigen-subchannels to encode messages based on Wishart matrices' Eigen values.

In a non-regenerative MIMO two-way untrusted relay system, authors of [265] have investigated a secure precoding design and applied AN on the source and relay is assumed to be untrusted. On the maximum secrecy sum rate, authors have also provided an asymptotic analysis. For the PLS of a multi-user Beam Division Multiple Access (BDMA) massive MIMO system, authors of [266] designed robust AN beamforming scheme with consideration of channel estimation errors.

Authors of [267], have proposed an effective adaptive selecting transmission mode scheme that maximizes the sum secrecy outage capacity. In the transmission of signals between the source and multiple secure users in MIMO Rayleigh fading channel, authors of [267] used harmful interuser interference as a tool for anti-eavesdropping. In [222], authors proved the guaranteed secrecy performance for MIMO HetNets in physical layer and derived upper bound secrecy outage expressions for a HetNet user.

MISO relay cooperative scheme for a near and a far vehicle has been studied in [131]. CJ protected zero techniques and an signal superposition has been adopted. Authors have proposed a optimal secure transmission scheme after careful analysis for eavesdropping security threats and two scenarios; i) optimized SOP to minimize message leakage with considerable rate of transmission. ii) improved averaged secrecy rate by providing a power allocation scheme with keeping system throughput into consideration.

For a finite memory Gaussian MIMO wiretap channel, authors of [268] studied the secrecy capacity subjected to per symbol power constraint. In [269], authors have proposed Advantage Distillation (AD) scheme for secret key sharing in MIMO wiretap channel using Generalized Extended Space-Time Block Codes (GEO-STBCs) and the feedback bits from the receiver. For the proposed scheme, authors have constructed Two-Way MIMO Wiretap With Feedback (TW-MIMO-WTF) channel.

Various authors used power allocation schemes to provide network security. In [270], authors have proposed a Joint Relay Selection and Power Allocation (JRP) scheme for improving the PLS of the network with untrusted two-way relay cooperative communication and passive eavesdroppers (non-colliding and colliding) with multiple antennas at the source and single destination antenna. In the proposed scenario, destination is implemented the CJ. For a secure communication, authors of [271] used an iterative algorithm to propose an iterative distributed total Mean Squared Error (MSE) minimization algorithm (MT-MSE). In [272], authors have investigated a power-ratio-based active pilot attack detection scheme in the underlay spectrum sharing multi-user mMIMO systems with active eavesdroppers and derived the probability of detection and MMSE channel estimation.

For a spatial Modulation (SM) MIMO system physical layer encryption, authors of [273] have proposed an encryption scheme called Chaotic Antenna-Index Three-Dimensional Modulation and Constellation Points Rotated (CATMCPR). The proposed scheme is based on spatial modulation and chaotic theory. The proposed technique overcomes the drawbacks including degradation of spectral efficiency performance, necessity of pre-shared key, excess jamming power, and requirement of prior CSI.

E. Channel Coding for PHY Layer Security

Channel codes are typically designed to make communications reliable by adding redundancy into transmitted data that allow for error detection and correction at the receiver. Channel coding is also typically the last encoding rule prior to transmission, thus preventing the propagation of errors at the decoder. A multilayer security solution for digital communication systems is provided by considering the joint effects of physical-layer security channel codes with application layer cryptography. Low Density Parity Check Codes (LDPC) and Polar codes are the candidate channel coding techniques proposed for 5G.

Some ciphers can be very strong when the code design guaranteed an insignificant error rate. In [274], authors exploited a point of failure in message passing decoding called stopping sets, for security. In [212], an AN-aided polar coded algorithm has been proposed to improve the secrecy requirement of the already existing polar coding algorithm as per requirements of upcoming 5G technology. The proposed technique is based on two steps. Initially, in the codeword of current transmission, AN noise from the previous transmission's code block confidentiality bits have been added. Hence, it can be removed by legitimate user only. The length of AN is shorter than the exact codeword, which deteriorates eavesdropper's receiving capability by optimized jamming position selection.

F. Secure RF Energy Harvesting

With the rapidly growing number of connected devices, the demand for energy is also rising exponentially. This results in upraising interest for QoS guaranteed energy-aware communication techniques to minimize the consumption of fossil fuel [275]. This reflects directly on the revenue of the mobile operators and other service providers as well. As there is no free-lunch this also comes with greater challengers such as secure transmission of data. RF Energy Harvesting (EH) techniques such as Wireless Power Transfer (WPT) and Simultaneous Wireless Information and Power Transfer (SWIPT) are received significant attention as sustainable techniques for EH [276]– [277].

The secret communication is conceivable when the eavesdropper channel is a worst than that of the destination channel. CJ aided secure communication for SWIPT networks was investigated in [278]. Here the jamming signal is used to reduce the eavesdroppers channel quality. Thus it helps the source to escalate the EH by the energy receiver. In [279] studied relative secrecy analysis of the separated and integrated receiver [280] architectures under imperfect channel estimation with SWIPT. This work emphases on the evaluation of secrecy performance of a SWIPT system with the combinations of receiver architectures at the legitimate receiver and eavesdroppers. Then, in [281], authors proposed a multi-antenna energy-constrained cooperative relay network in the context of physical layer security using SWIPT. A new SWIPT protocol referred as harvest-and-jam was proposed in [277] to maximize the secretary rate for a self-sustainable mobile BS setup.

G. Other Physical Layer Issues Related to 5G

To address the PLS in mmWave network authors of [282] have proposed a beamforming approach called Frequency Diverse Array (FDA). The proposed scheme introduces a frequency offsets across antenna array to decouple the high correlated channels of users and eavesdroppers. In [283], authors proposed a multiple inter-symbol obfuscation scheme, which depends on AN symbols. This scheme protects the transmission from the passive eavesdropping and package injection attacks.

Authors of [284], proposed an Opportunistic Relay Selection (ORS) scheme to provide high Security-Reliability Trade-offs (SRT) in the presence of eavesdroppers. Authors of [285] have proposed a user cooperation scheme based on Weighted Fractional Fourier Transform (WFRFT). In the proposed technique, cooperators information signals can introduce AN effect on eavesdroppers. Authors modeled a cooperation problem as a coalitional game for WFRFT-based PHY-layer security with non-transferable utility. Authors of [286], claimed to improve the Primary Users (PU) security with the help of Secondary Users (SU) transmission interference in a cognitive radio (CR) network. In traditional schemes, SU is harmful for PU. In the proposed scheme, authors shared the spectrum between SU and PU; however, primary user can demand the high spectrum to achieve high secrecy capacity. In [287], authors have proposed a game-theoretic framework called Multi-hop Topology Formation Game (MTFG) to provide joint optimization of PLS with end-to-end delay management in the Wireless Body Area Networks (WBANs). In the proposed framework, along with fulfilling the E2E delay requirement body-worn sensor devices communicate in the presence of fading and wiretap channel condition in order to find the safest multi-path hop to the destination.

In [213], three strategies i.e. Global-Defense Cooperative Anti-Eavesdropping Strategy (GD-CAES), Max-Min Cooperative Anti Eavesdropping Strategy (MM-CAES) and Delay-Aware Cooperative Anti-Eavesdropping Strategy (DA-CAES) were proposed based on the graph/secrecy Shortest Path Algorithm (SPA) technique. They are less complex than Hardworking path selection (HW-PS). The proposed techniques are subjected to three different scenarios including the cooperation among eavesdroppers with MRC of wiretapped signals, independent eavesdroppers with and without MRC. For less complexity of the system, greedy algorithm has been selected for an optimization problem solution.

VI. Security Monitoring and Management

This section presents the most important challenges related to security monitoring and management in 5G networks.

Network monitoring is an important network management aspect in telecommunication networks including 5G networks. These monitoring systems collect various information including network statistics, traffic patterns, application status and user profiles. In addition, these systems can collect the flow samples at various intervals and granularities. This information is useful to evaluate the status of the network as well as to perform various security and network management tasks such as anomaly detection, network forensics analysis, load balancing, traffic engineering, enforcing Service Level Agreements (SLA) and maintain QoS. Moreover, network monitoring is used for detection and prevention of security breaches, that will ultimately enhance the overall network performance [288].

Future 5G networks will connect huge number of devices (e.g., mobile phones, laptop and tablet computers, IoT devices, robots, drones, and automated vehicles) and it will exponentially increase the workload on security monitoring systems [289]. In addition, 5G has promised to offer enhanced consumers experience with powerful network performance and seamless experiences across many verticals. This requires the 5G monitoring systems to update by several challenges, such as monitoring E2E performance across complex architectures, delivering dashboards, reports, and alerts with speed at scale and ensuring multi-disciplinary 5G customers are satisfied with speed, performance, and their overall mobile experience.

However, the monitoring systems are incapable of handing this demand due to complex, distributed and uncoordinated system management, high provisioning and operational costs, lack of support for automation, hardware dependency and vendor-specific monitoring. Existing 4G monitoring systems do not have a centralized controller. Different monitoring systems have implemented at the different segments of the networks, e.g Deep Packet Inspection (DPI) at the eNodeBs, Security Information and Event Management (SIEM) at Evolved Packet Core (EPC). As the results, the network monitoring gets complicated. Current monitoring systems are heavy dependent on physical hardware. Furthermore, most of the monitoring mechanism are operating on the vendor proprietary hardware [290], [291]. Therefore, it is impossible for mobile network operator to upgrade or modify these mechanisms without the consent of the vendor. Due to the high dynamicity in 5G networks, this is one of the critical concerns for MNOs. Moreover, existing monitoring techniques in mobile networks are over-provisioned to work even at the peak hour traffic loads. Thus, most of the available resources are under utilized for a long period [290], [291].

Therefore, 5G needs more dynamic and scalable monitoring systems than current systems. In addition, 5G consists of both physical and virtual resources. Existing monitoring systems do not capable of monitoring such virtualized devices. Thus, there is a definite need to design new monitoring systems, which can monitor virtualized elements as well [292], [293]. On one hand, 5G network monitoring mechanisms should be able to satisfay the requirements introduced by the virtualization. On the other hand, they should be able to obtain benefits from the flexibility offered by SDN and NFV [291].

In SDN based 5G networks, the centralized control is allowing to create monitoring apps that can take decisions based on a network-wide holistic view. In such systems, the centralized event correlation is possible at the network controller. This allows design new ways and algorithms to mitigate network faults efficiently [291]. Similarly, NFV can be used to virtualize the existing monitoring solutions such as SIEM, IDS, IPS (Intruder Prevention Systems), DPI [294]. Moreover, NFV can improve the scalability of 5G monitoring applications by dynamically scaling increasing the monitoring resources according to the traffic demand. However, the impact of virtualization technologies has to be assessed. For instance, virtualization creates boundaries that could be breached by exploiting vulnerabilities and bugs in the virtualization code (e.g., hypervisors). Furthermore, the entire 5G systems actually become files store in some place that can easily be stolen or replaced [295].

Various architectural options were proposed for 5G monitoring systems. Fig. 23 and 24 illustrates the 5G software Defined Monitoring (SDM) architecture which was proposed based on SDN and NFV technologies [290], [291], [294], [295].

In [290], [291] authors as proposed a SDM architecture, which can be used in NFV enabled softwarized networks including 5G. Moreover, network monitoring frameworks for NFV are proposed in [294]–[297]. These architectures proposed to deploy both virtual and physical sensors in the different segment of the network. The network monitoring

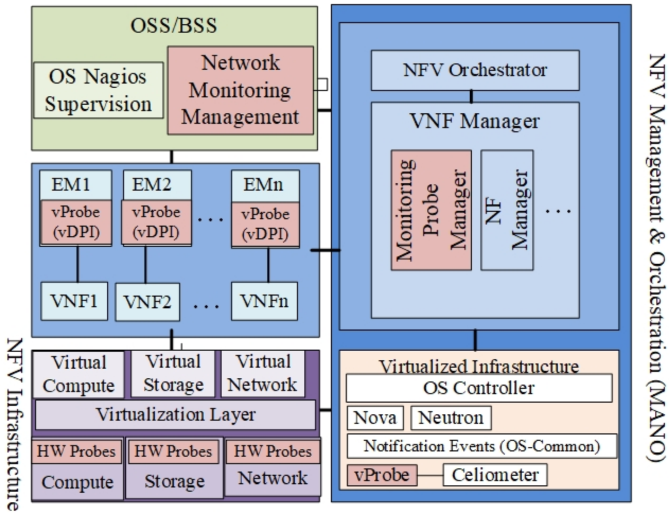


Fig. 23. 5G software Defined Monitoring (SDM) architecture mapping with NFV [290], [291], [294], [295].

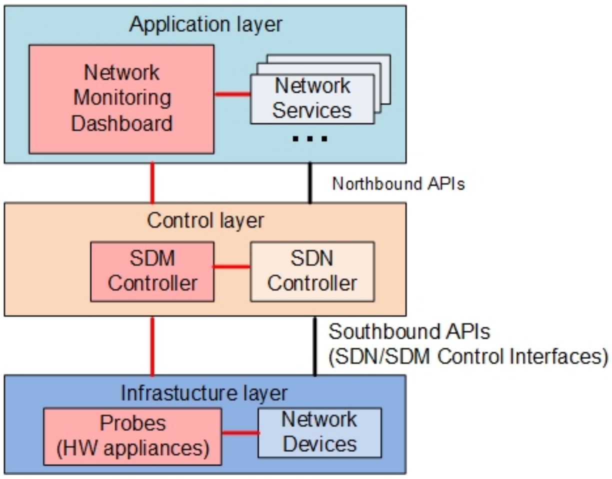


Fig. 24. 5G software Defined Monitoring (SDM) architecture mapping with SDN [290], [291].

management entity is mainly responsible for the management of network-wide network monitoring. Monitoring probe manager is responsible for the deployment of both virtual and physical probes across the network. Moreover, the existing NFV and SDN interfaces will be modified to enable new SDM Control Interfaces. This new interface uses to transport the packet flow data and meta-data needed by network monitoring applications and Network Services modules. This data will be transported from either the switches or the probes (i.e., agents) to SDM controller. By introducing SDN-driven SDM, SDN-enabled switches, COTS packet processing and security appliances can act as packet brokers [298].

Table X presents the limitations in legacy monitoring techniques and the possible solutions proposed by SDM.

In [301], authors proposed an 5G-oriented automatic monitoring management architecture. This architecture integrates both SDN and NFV concepts to monitor and orchestrate the whole life-cycle of monitoring services in 5G networks by considering control plane information. A novel IoT based network monitoring framework for 5G mobile network was proposed in [302]. The proposed framework simplifies the implementation of the monitoring system for 5G network operators.

TABLE X
LEGACY MONITORING TECHNIQUES VS SOFTWARE DEFINED MONITORING [290], [291], [294], [295], [299], [300]

Limitation in Legacy Monitoring Techniques	**How SDM Can solve it**
Difficult to deploy and maintain	Simplifies network management and maintenance via network automation
Distributed infrastructure	Centralized control of monitoring functions via monitoring controller
Difficult to automate mitigation actions	The network softwarization enable the ability to automates mitigation actions.
Independent resources	Virtualization enable the sharing of resources between different services in the network
Under unitized resources	The sharing of resources between different services is offering the opportunity to optimize the utilization of network resources
Redundant Monitoring	The centralized coordination can eliminate the redundant monitoring in the network
Vendor dependent monitoring equipment	Open network standards eliminate the requirement to use vendor specific equipment
High CAPEX	Vendor independent equipment, optimization and sharing of resources reduce the CAPEX
High OPEX	Automation of network monitoring, optimization and sharing of resources reduce the OPEX

Moreover, some of the other technologies such as machine learning are used for SDM architecture. In [303]–[308], authors proposed to used machine learning algorithms for anomaly detection in vitalized networks. Proposed solutions can achieve high precision and low false alarm rate than tradition approaches. A survey on SDN based network intrusion detection system using machine learning approaches is presented in [309]. An efficient deep learning model for intrusion classification and prediction for 5G and IoT networks was proposed in [310]. Authors evaluated their model by using the benchmark Aegean Wi-Fi Intrusion data-set and the proposed scheme had 99.9% overall detection accuracy of for Flooding, Impersonation and Injection type of attacks. A novel DDOS attack detection scheme for 5G was proposed in [311]. Here, the traffic flows are inspected at source-side looking for discordant behaviors.

On the other hand, there are new challenges such extensible and programmable instrumentation, measurement data analysis, visualization and middle ware security features which are rated to softwarized network monitoring systems. In [312], authors discuss such research challenges related to the performance measurement and monitoring of the future virtual network. In [288], [290], [291], authors highlighted the challenges such as compatibility with traditional monitoring systems, complex monitoring applications, scalability and performance challenges, placement of the monitoring controller, adapting traditional monitoring techniques to SDN and information extraction related to SDM. In [288], authors surveys the tasks and challenges associated with network Monitoring in SDN which are also quite relevant to 5G networks.

VII. Privacy in 5G Network

5G networks promise to serve the end users with smart services which will raise many privacy issues from the viewpoint of users. The services offered in 5G network will contain primary information (such as identity, location or position, and private data) about its users. How this information will be stored and in what conditions individual data can be available by many stakeholders, therefore, 5G networks evoke significant issues on private-data leakage. In this section, firstly, we focus on privacy categories from the view point of the users , secondly privacy issues in 5G network, and finally privacy goals under the 5G network architecture.

A. Privacy Categories From the Users Perspective

This subsection discusses three different privacy categories i.e. data privacy, location privacy and identity privacy [313], as follows.

- **Data privacy**: 5G networks allows users to use smart and data-intensive on-demand services (e.g., high-resolution streaming, healthcare [314], smart metering [315].) through the heterogeneous smart devices. To provide these services, service providers may store and use private data of individuals without their permission. The stored data may be shared with other stakeholders so that they can analyze the data using Machine Learning Techniques (MLTs) and find new business trends for their own product, which could be more suitable for that user. For instance, recent studies pointed out that a smart meter consumption data may reveal personal information, e.g., a house is empty or economic status. To mitigate such data privacy issues, service providers must provide the clarification for the users that for how and where the individual's data have been stored. In addition, how and what purpose their data have been used.
- **Location privacy**: In 5G network, most devices will rely on ubiquitous Location-Based Services (LBSs) [316]. A LBS uses location data, which is related to the smartphone and/or mobile device to deliver services to the users. Recently, the promotion of LBS has significantly increased in several verticals, for instance, government, entertainment, transportation, healthcare, food delivery and others. Indeed, such LBSs make users life easier and more enjoyable but bring plethora of privacy issues that of being continuously tracked. In some cases, the individuals may be unaware of the potential risks graveled by these technologies and the implications of how their location is being determined, and who is being permitted access to that information. More importantly, recently, digital media reported telecomm companies are revealing the exact location/position of their users to several stakeholders without the users consents. As a consequence, LBSs could case potential risks to users privacy.
- **Identity privacy**: It means the protection of identity-related information of a device/system/user against active attacks. As more and more devices are being connected to the Internet, it raises alarming conditions of identity theft [317]. For instance, in recent research, the authors have pointed out that the active attacker can expose the identity of a subscriber by catching the International Mobile Subscriber Identity (IMSI) of the subscribers UE [24]. Moreover, the more details can be found about a user through the identity theft. Identity theft can therefore be counted as one of the biggest risks in the 5G and IoT. Thus, it is paramount to design secure and efficient identity management mechanisms for the identity privacy in 5G network.

B. Privacy Issues in 5G Networks

The 5G networks are going to be very vast networks including several stakeholders, new technologies, verticals, businesses, regulations, and end-users. Covering privacy issues for each stakeholder is a complex task because multiple interests are at stake. However, few of privacy issues are pointed out below from the cloud computing point of view. This is due to the fact that cloud computing concepts are relevant to many of 5G network technologies, such as SDN, NFV [313].

- **End-to-End data privacy**: 5G networks support several stakeholders such as operators, service providers, verticals, enterprises, and new technologies in conjunction with new business models. Most of these stakeholders make use of cloud computing to store, use and process personal information from the consumers. The personal data of the consumers will be processed and shared by different stakeholders their own purposes, thus this become a source of privacy breaches. Therefore, in 5G networks must consider an end-to-end data confidentiality approach to protect the consumers privacy [25] [10].
- **Shared environment and loss of personal data ownership issues**: The 5G network would provide shared network infrastructure or virtual networks to run multiple applications controls, such as healthcare and smart grid. Such shared network infrastructures may pose unauthorized data access and exchange as shown in [318]. Therefore, effective solutions are needed that can offer shared network infrastructure functionalities without compromising the privacy of the users. Moreover, in a shared network infrastructure, assume if the personal data losses then who will own the responsibility, which is a big concern among the users. Therefore, the ownership or licensing of personal information must be assigned/defined between the stakeholders such as mobile network operator, service providers and third-parties.
- **Different trust objectives issues**: In a typical 5G network, mobile operators and communication service providers may collaborate and migrate a portion of their network to cloud. In such circumstance, these stakeholders may have distinct trust objectives/priorities as per their own policies and/or regulations [313]. Hence, they might not necessarily consider all aspects of privacy of the consumers data.
- **Issues in trans-border information flows**: Due to the global digitalization, personal data is a lifeblood of the modern market and it will freely flow across the borders.

As data freely flows, it is highly paramount to mandate individual or government consent for the data transfers including how information is being processed and stored across the border [313] [319].

- **Third party issues in 5G network**: 5G with IoT brings a new frontier for the application developers to design more interactive applications for the several vertical applications those utilize several communication protocols. As the application designers are typically granted permissions to access the 5G network, he/she may disclose or sell individual's private data to other entities. For instance, as shown in [320] – "the health insurance portability and accountability act (HIPPA) allows a share-out of individual's health data" by using mobile apps. Moreover, the information sharing rule in a cloud network can significantly invoke data-privacy issues.

C. Regulatory Objectives in Privacy Protections

Regulatory objectives are paramount to achieve privacy in the 5G domains. As the 5G networks research is at early stage, not many direct objectives are defined by the regulation bodies. However, few generic regulatory objectives from the cloud computing [313] can be extended to 5G networks, as follows.

- **Single market promotion and balance the interests globally**: Single market promotion refers to all the relevant regulatory objectives or legislative practices should be promoted to strength and enable privacy policies globally without any internal borders and regulatory obstacles. In addition, the privacy regulations should balance the interest of different stakeholders including the consumers in order to realize the benefits of 5G technologies and its applications.
- **Promote data portability**: The principle to data portability allows the individuals/businesses to shift their personal information from one service provider to another service provider, and from one country to another country without employing mandated standards [321] [322]. Therefore, it is highly needed to promote data portability in 5G networks.
- **Define global market privacy regulations**: In the context of a global market, new data privacy regulations are required to ensure interoperability and compatibility with the 5G based technology. Globally, different regulation bodies must collaborate and cooperate to each other, and develop requirements for the new privacy regulations. For example, the EU-US Privacy Shield, enforces responsibilities on the US companies to keep secure private-data of the EU citizens [323].
- **Promote data accountability and responsibility**: As the several players will involve in the 5G network, the data accountability and responsibility are highly required. The accountability act involves different stakeholders to take obligations for *how and when* they will use individual's private data and *what* rules will be followed when the data is accessible to other stakeholders [313]. Therefore, all the stakeholders must have significant and appropriate measures in place that can prove accountability and responsibility for the personal data.

Table XI shows the impact and relevance of regulatory objectives with privacy issues.

TABLE XI
IMPACT AND RELEVANCE OF REGULATORY OBJECTIVES WITH PRIVACY ISSUES [313]

	Single market promotion	Data portability	Global market regulations	Data accountability
End-to-end data privacy	×	×	×	×
Shared environment issue		×	×	×
Trust objectives issues	×	×	×	
Trans-border information flow	×		×	
Third party issues	×			×

D. Privacy Mechanisms

Following the new EU General Data Privacy Regulation (GDPR), individual privacy is an important issue for all the stakeholders those are gathering and using individual's personal s data [324]. Therefore, it is paramount to use efficient algorithms, schemes, and protocols that will protect as much as possible user information. From the perspective of 5G networks, many of distributed applications and devices (e.g., healthcare, smart grid, mobile, IoT devices, sensors and actuator) exchange messages across their network via communication technologies and protocols. Such applications and devices significantly expand a huge number of messages (e.g., high-resolution streaming, smart metering, and so on) over the Internet. However, the main question is how these messages will be collected, stored and used without disclosing the private-data of individuals. Moreover, key privacy properties can be used in 5G network, as follows.

- **Anonymity**: In this property, an object is not capable of being identified among its peers (i.e., in anonymity set) [325]. An end-to-end anonymity aims the identity of an entity is being hidden from others, even in a same anonymity set.
- **Unlinkability**: In unlinkability, the individual's information is usually unlinkable between two or more users in a system. In the evolving 5G network, unlinkability is highly important and it can be enforced at various domains in the 5G networks, such as SDN, VPN, routing, and back-end servers (i.e., data aggregators, cloud servers).
- **Undetectability**: In 5G network, several objects (such as, machines, applications, users.) will communicate and exchange information between each others. However, an attacker may have an interest to detect the communicating entities by eavesdropping on information/data exchanged [326]. Therefore, in 5G network the information and/or objects must be undetectable to the attacker.
- **Unobservability**: In this property, an attacker may not be able to observe whether two or more entities are

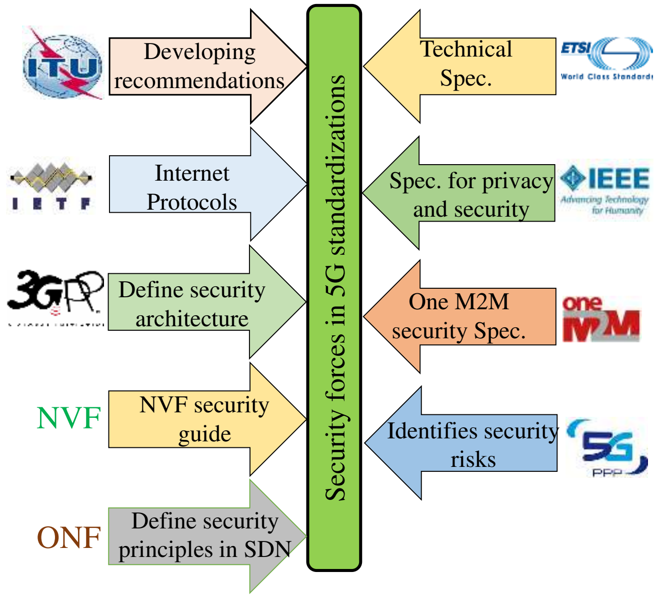

ITU
Developing recommendations
IETF
Internet Protocols
3GPP
Define security architecture
NVF
NVF security guide
ONF
Define security principles in SDN
Security forces in 5G standardizations
ETSI World Class Standards
Technical Spec.
IEEE Advancing Technology for Humanity
Spec. for privacy and security
one M2M
One M2M security Spec.
5G PPP
Identifies security risks

Fig. 25. 5G standardization security forces and their role.

participating in the communication [325]. In other words, if an entity had sent a message over the communication then an adversary (i.e., active or passive) should not be able to observe the targeted entity, such as sending mobile healthcare data to the physician.

- **Pseudonymity**: A pseudonym is an instance of an object that is unlike than the objects real names. In the 5G networks, typically several stakeholders will be involved. As these stakeholders can access the personal information, a smart object must have several instances (i.e., pseudonmity). These instances are only be known by the involved entities those are exchanging information with the smart objects.

VIII. 5G Security Standardization

With the advent of 5G, standards are particularly paramount globally. Typically, a standard is a key for the convergence of telecommunication and IT sector to develop a ubiquitous infrastructure. Such ubiquitous infrastructure will offer global services to customers and create new opportunities to interconnect a wide range of smart objects. To ensure the 5G promises, all security events or issues going with the 5G architecture need to be handled in a standardization way. However, as the 5G is under development, the security standards for the 5G networks are still the drafting phase.

Globally, there have been a big number of standardization bodies those are contributing immensely defining security requirements. Nevertheless, these bodies provide security recommendations and specifications in 5G network, as shown in the Fig. 25. Moreover, these standardization organizations are working on security issues and solutions in 5G network. In addition, few of the groups are also accountable for the economic regulation of the telecommunications sectors, and supervising technical interoperability and safety of the 5G networks in their respective countries. In addition, a number of local governing bodies are trying to regulate the security mechanisms in a certain local area.

In release 15 [230], 3GPP defines a security framework, architecture and possible operations for the 5G systems. Particularly, the security architecture has been proposed for different domains in the 5G networks, e.g., security at the network level, security for end-users, security for the applications. The architecture introduces of several security entities, such as AUSF, Authentication Credential Repository and Processing function (ARPF) and Security Anchor Function (SAF). In addition, the document defines general security requirements, e.g., key management, authentication and access control, data confidentiality and integrity, and privacy for the subscribers. For details, the reader may refer to [230].

International Telecommunication Union (ITU), collects input from many local organizations and defines high quality technical recommendations that are easy to implement in the 5G networks [327]. However, the study group 17 (SG17) is mainly responsible for designing and developing security in the use of ICT. In order to better understand 5G threat landscape and security requirements, the SG17 is closely collaborating with the 5G manufacturers, telecommunication operators, regulators, and application providers [328]. The security group is not only focusing the traditional threats but also considering the possible threats from the quantum computers, which are yet to happened. However, few of the security requirements (e.g., access control, authentication and encryption) have been considered for the SDN, NFV, and network slicing.

5G is set to be a faster broadband that is connected with Internet and Intranet protocols, therefore, the IETF is expected to play a key role. Note: the IETF has not commenced new contributions to major items that can be specifically labeled for the 5G network. However, many of existing Request For Comments (RFC), such as IP Wireless Access to Vehicular Environments (IPWAVE) WG [329] and Host Identity Protocol (HIP) [330] can be directly used in the 5G networks. The Authorization for Constrained Environments (ACE) WG is working on authenticated authorization protocols for gaining resources hosted on servers in low-powered environments [331]. In addition, recently, Kumar-verma suggested an IETF draft ”Security for 5G”. The authors proposed a new technique that can mitigate several issues of attack over the mobile communication system [332]. The draft proposed to use a public key cryptosystem to encrypt the mobile communication traffic. However, in order to realization security in the 5G network, such drafts are at early stage.

European Telecommunications Standards Institute (ETSI) has identified technical specifications, e.g., ABE as a key enabler technology for distributed systems in 5G networks. ETSI technical commission of cyber security has issued two access control specifications (i.e., ETSI TS 103 458 [333] and ETSI TS 103 532 [334]) for 5G networks. ETSI TS 103 458 focuses on how to secure user identity, and preventing disclosure to an unauthorized entity in a WLAN and cloud. Whereas ETSI TS 103 532 describes trust models protocols using ABE mechanism and increases data security and privacy in untrusted environments. In 2016, ETSI specifies the security and trust guideline for the network function virtualization (NFV) security [335]. NFV security-group has highlighted the need for trustworthy models that can maintain trust within VNFs and between VNFs. In 2014, the ETSI MEC ISG (Industry Specification Group) was organized for aiming of standardizing the MEC environment. In addition, the working group has also been responsible for determining different possible service use-cases, and for defining technical requirements for MEC.

Institute of Electrical and Electronics Engineers (IEEE)-P1912 provides specifications for privacy and security architecture for the end user wireless devices [336]. The specifications are issued for the Home Area Network (HAN), Wireless Area Network (WAN), and Wireless Personal Area Network (WPAN). The architecture mainly focuses on simplification of user authentication. Other standards in IEEE include 802.11, where a secure interoperability and mobility are provided with the outer world. In the 5G network, many of security standard can be adopted from other groups, for instance oneM2M (Machine To Machine). The security architecture in oneM2M consists of several layers: (i) security functions layer, (ii) security environment abstraction layer, and (iii) secure environment layer [337]. The main security attributes in oneM2M are authentication, authorization, and identity management.

The 5G PPP security working group was established in early April 2016 and led by 5G-ENSURE [338]. The heterogeneous nature of the 5G infrastructure, may result in unauthorized and opportunistic access or usage of assets. The group therefore identified many security-related risks including 5G Identity thefts or cloning, unauthorized access of 5G connected devices critical data. In addition, new threats due to their seamless inter-working as requested 5G. Following the risks, a new security architecture for 5G has been suggested in [338].

There are various other suitable standardization bodies (such as, Trusted Computing Group (TCG) and Open Networking Foundation (ONF)), which are closely collaborating to the 5G networks. At TCG, the Mobile Platform Work Group (MPWG) develops application scenarios, platform frameworks and examines the security of 5G network [339]. The ONF typically recommends to make use of SDN and network operating systems in the applications and industrial verticals [340]. The specifications of the ONF, including OpenFlow tool, can be a mainstream tool for the 5G core architecture. Consequently, these specifications and tools are imperative from the security perspective in 5G networks.

Next Generation Mobile Networks (NGMN) 5G Security Group – the NGMN Alliance typically refers a mobile telecommunications association [341]. The alliance is comprised of many entities, such as mobile network operators, service providers and device manufacturers. The security group objective is to guide standardization and implementation of 5G security features. The group produces 5G security related high-level requirements and recommendations. Moreover, the group concentrates on enhancing the communication infrastructures via incorporating the LTE-advance networks that included various platforms to advance mobile services in 5G. Moreover, NGMN 5G security group has published a document on 5G security, MEC, low latency, and consistent user experience [342]. Basically, the document defines several service scenarios and technical requirements for MEC in 5G.

National Institutes of Standards and Technology (NIST): is playing an important role in the standardization efforts of 5G technologies, e.g., cloud computing (CC). The group is known as NIST CC. The main agenda of the group is to design and accelerate the secure cloud computing to the 5G network. Through standard developments and guidelines, the NIST is closely collaborating with the federal official, government and standard bodies [343]. Moreover, the NIST CC group designed and developed a high-level conceptual model and reference architecture for cloud computing. This reference architecture includes relevant requirements and other procedures of cloud computing in the 5G networks.

In summary, the standards and specifications that will define a mature and complete reference architecture for the 5G network are yet to be finalized and outlined. It may take many more years and involve several stakeholder entities involving service operators, governments, regulators, manufacturers, policy-makers and representatives of 5G users. Nevertheless, enormous academic research and standardization are still ongoing activities in the 5G networks.

IX. Projects

This section presents some significant ongoing research projects that are explicitly contributing to 5G Security efforts. The presented projects along with their technical contributions are summarized in the Table XII.

TABLE XII
Contribution of Global level ongoing projects

Technologies	**5G PPP**	**5G Ensure**	**NSF**	**STEAM**	**ANASTACIA**	**5G! Pagoda**	**5G-MiEdge**	**5G Champion**	**IRACON**	**RECORDIS**
MEC	√	√	√	√	√		√			√
IoT	√	√	√	√					√	√
SDN	√	√						√		√
NFC	√	√	√	√						√
Network Slicing	√	√	√			√				√
mmWave	√	√					√			
NOMA	√	√								
massive MIMO	√	√	√						√	
D2D	√	√							√	
UAVs	√	√								
Full Duplex	√	√								
OFDMA	√	√	√						√	

A. European 5G PPP [5G Infrastructure, Public Private Partnership] (2013 - 2020)

This is a platform for public, a joint initiative between the European Commission and European ICT industry. The 5G PPP initiative was initiated based on the experience of ICT infrastructure and communication networks. This consortium will be empowering the global competitiveness of European industry. This created the platform for creating new opportunities for a new PPP action on networking infrastructures [344]. This offers funding and support for 5G related SMEs (Small and Medium-sized Enterprises) and other related projects to foster and realize the EU commission's 5G vision.

Security challenges faced by the ICT industry and the solutions for those challenges would be valuable for the future PPP projects. Security solutions gained by the experience of ICT industries are invaluable and provide opportunities for the new entrants in the industries. Those new entrants could be small start-up companies incubated from Universities and other research institutes. New startup companies are vital for PPP and they bring new ideas, most of the leading companies like Skype and TransferWise are developed from the startups. The security solution provided by the new entrants (start ups) for the 5G infrastructure and communication networks can be more specific based on the feedback from the peer industry. Thus, the European 5G PPP would be an excellent and more suitable platform for the collaboration between ICT industries, Government and the new entrants. This partnership leads to the capacity building of the EU in 5G and their future innovative ideas will be resourceful.

B. 5G Ensure [Enablers for Network and System Security and Resilience] (November 2015 - October 2017)

This initiative aligns with the 5G PPP and introduces a road map for achieving 5G security targets at the European scale. This action will define challenges in relation to 5G security. This project introduces 5G basic architecture and other main concerns along with security goals [345]. They also focus on other trends such as network deperimeterization and software defined networking and virtualization. The security architecture builds on and expands on the 3GPP security architecture.

C. National Science Foundation Programs Funded 5G Security Projects

National Science Foundation (NSF) Programs of US fund many ICT research projects and it has certain programs that focused on cybersecurity [346]. Some of them are listed below:

1) Secure and Trustworthy Cyberspace (SaTC)
2) Information and Intelligent Systems (IIS)
3) Networking Technology and Systems (NeTS)

5G security plays an important role in the ICT industry because 5G communication is going to be an integral part of ICT. Thereby, many future research projects are specifically focused on 5G communication and its infrastructure [347], which are part of the 400 million USD initiative [346]. Funding for 5G security projects are approved by the NSF under the categories SaTC, NeTS and IIS. SaTC program is solely dedicated to support projects that strive for national defense and ICT security. The programs like IIS and NeTS are robust programs dedicated to technological advancement like AI, automation etc. In cyberspace, which includes ICT and its security aspects. For example, under the NeTS program, funding is awarded for projects related to the IoT security as in [348], likewise there are many other projects are supported by NSF. These programs provide opportunities for the research institutes and project principal investigators affiliated with the USA based university.

D. STEAM [Secure and Trustworthy Framework for Integrated Energy and Mobility] (September 2018 - August 2021)

Secure and Trustworthy Framework for Integrated Energy and Mobility (STEAM) in Smart Connected Communities [348]. STEAM is a collaborative project, which is funded by the Japan-US Network Opportunity 2 (JUNO2) and NSF. JUNO2 program is specifically focussed on research and development of trustworthy networking for smart and connected Communities. Under the collaboration, STEAM project utilizes data from the Japan automotive sector and, also access tested and other infrastructure from Japan. With this realtime data and tested, STEAM will develop an innovative algorithm that sloves the security and privacy issues of smart meters, energy exchange and resource allocation for the ICT related applications. Finally, they will design a modular, secure and trustworthy middleware architecture that implements the innovative algorithm on the ICT applications in the Japan automotive sector.

E. ANASTACIA [Advanced Networked Agents for Security and Trust Assessment in CPS / I0T Architectures] (January 2017 - December 2019)

The aim of this project is to develop a new paradigm with new methodology and tools to increase security and privacy, reliability in a dynamic and rapidly evolving environment [344]. The research and development are focused on providing a holistic solution that enables trust and security for Cyber Physical Systems (CPS) and cloud architectures.

ANASTACIA will develop an adaptation trustworthy autonomic security framework for an entire ICT Systems Development Lifecycle (SDL). The framework is adaptable in the sense, that it allows diverse enablers in the ICT system to dynamically organize and deploy user security preferences and facilitates the deployment and enforces the security frame in heterogeneous scenarios which includes the system based on NFV, SDN and IoT networks. ANASTACIA will ultimately facilitate the security analysis along with the solutions for the positioned gears with simple and customer friendly security policy tools.

F. 5G! Pagoda (July 2016 - June 2019)

The pagoda is a Japan and European collaborative project that focus on developing scalable 5G slicing architecture, that evolves from the current NFV architecture towards an architecture that support of different specialized network slices composed of multi-vendor virtualized network functions, and considering interoperability within/among the network slices as well as with legacy system-based services [349]. The architecture accommodates scalable, flexible and dynamic network slicing concept while addressing many security aspects like risk management, privacy and secure society.

G. 5G-MiEdge [Millimeter-Wave Edge Cloud As an Enabler for 5G Ecosystem] (July 2016 - June 2019)

5G Millimeter-wave Edge cloud as an enabler for the 5G ecosystem (5G-MiEdge) is a three-year collaborative research project with eight partners. This includes ICT industries and universities [350]. It is co-funded by the EU and Japan. The project develops transmission schemes and protocols of mmWave access and backhaul for assisting mobile edge cloud with prefetching and caching, which helps to realize ultra-high speed and low latency service delivery. 5G security frameworks and protocols are considered in the project in order to enable a secure orchestration of communication and the computation resources of the mmWave edge cloud. The 5G-MiEdge project will use to demonstrate 5G and beyond features in testbeds in the city of Berlin, and at the 2020 Tokyo Summer Olympics.

H. 5G Champion [Communication with a Heterogeneous, Agile Mobile network in the Pyeongchang wInter Olympic competitioN] (May 2015 - September 2018)

This is a collaborative project of European and South Korean partners, that comprises ICT industries and research institutes [351]. The project developed enabling technologies that were already showcased as a proof of concept at the 2018 Winter Olympics in PyeongChang, South Korea.

In this project, one of the main project package is to develop a secure novel security protocol to use NFV/SDN. Advanced evolved packet core solutions for efficient system management with virtualization were developed that uses NFV/SDN in a secure backhaul architecture as well as a novel SDN-based Internet protocol security (IPsec) tunnel architecture.

I. IRACON [The Inclusive Radio Communication] (March 2016- February 2020)

IRACON is a COST action EU project on 5G with participation from mainly European participants and funded by COST association and EU [352]. IRACON developed an ecosystem that helps the partner to access experimental facilities of within the consortium by sharing resources such as connected cards, ehealth, factories of the future and energy management. This project has a wide spectrum of research interest such as Radio Access, IoT, Over-The-Air testing, PHY, NET, IoT for Health and Localization and tracking. In most of working groups consider security aspects of their respective research domain.

J. RECORDIS [Resilient communication services protecting end-user applications from disaster-based failures] (March 2016- February 2020)

This project, is a European level consortium, is to introduce the techniques of resilient communications, as well as suggestions on how best use and develop communication techniques to support disruptions and relief operation at European level. This action offer wide range of solutions to provide resilient communications to overcome all types of disaster-based disruptions in networks such as IPv4-based, current Internet, and future internet and networks.

X. Lessons Learned and Future Directions

5G communication security is a hot research topic. There are many open research areas with high levels of challenges that needs to be tackled in a sophisticated manner. Providing new solutions must be bounded with certain requirements and restrictions like low complexity and reliability. This section briefly discusses lessons learned from related work and possible future directions for several 5G security communication systems.

A. Mobile Network Security Landscape

1) Lessons Learned: It is noticeable that the security challenge according to the provided 5G security landscape is extremely high. A lot of research challenges due to new technological enhancement have been observed. Along with the ongoing stuff, it has increased the risk of threats especially for cybercrimes, political and personal threats. New threat protection model based on CIA will be useful. Some centralized policies may also be helpful to control the access of the overall system. However, this is not enough at all. There are a lot of security threats that requires special attention before the implementation of 5G.

2) Future Directions: For the implementation of 5G communication landscape, requirements of amendments lead in various future directions in the system. The details of the types of attacks are given in the section II. Fig. 26 gives a brief overview for the types of existing and new types of attacks as a brief overview of future work. Fig. 26 also lists the possible attacks on centralized policy and visibility. All type of attacks need equal attention to provide a secure landscape in the advanced technology.

Along with the existing technologies, IoT is a new technology where all the devices are connected with each other in the form of the completely smart world. For IoT security there are a lot of open research areas including the establishment of high accuracy detection for mobile malwares and the Zero-day detection. A number of authors intend to intend to enhance IoT security for 5G communication system. Authors of [353] aimed to create a secure system for different CPANs and their secure network management. With the developed component authors of [77] offers to improve the authorization, authentication and other basic goals particularly for IoT. Implementation of AI will be helpful in providing fast authorization, authentication and trust development between each IoT device. AI system security will perhaps provide high system security. In addition to the research of security system with AI, researchers must also consider the security threats based on AI.

B. Security Challenges in the Access Control

1) Lessons Learned: There are a number of techniques proposed to improve the access control. Due to high and decent demand for 5G technology, the existing work is not sufficient as we believe that the content access requires access rights and authentication from an always-online server, which is quite difficult in many of 5G use-cases. In addition, access right

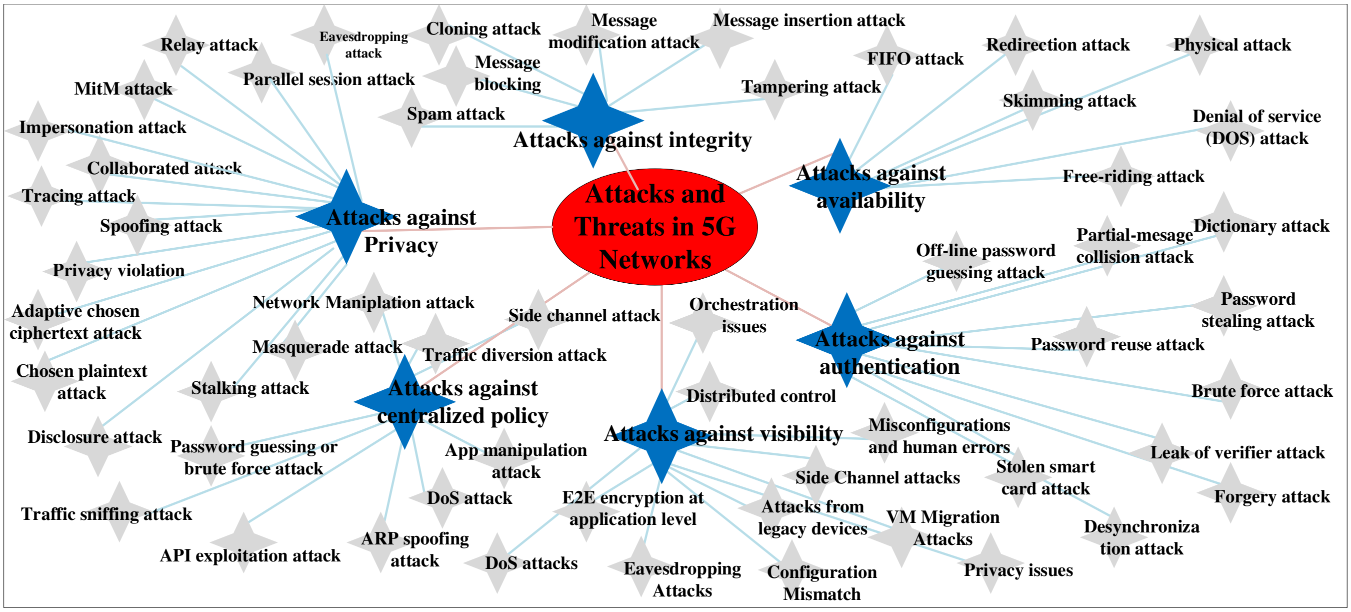


Fig. 26. Types of Evolved security Threats for 5G Networks.

revocation is an another issue of the state-of-the-proposals. Hence, the access control needs a proper attention especially in terms of its security, access rights and access revocations. It must also be noted that the requirement of quick access to the system will be important especially in industries and hospital in terms of IoT technology. Therefore, the access to the system must not be critical, delayed and fulfill the security requirements.

2) Future Directions: Researchers provided some of the new solutions in this area. As a future work the technique proposed in [128] can be improved to decentralized group initialization. According to [128], the JSS protocol efficiency can also be improved in terms of communication and the requirement of a reliable communication channel. Noticeably, a lot of work for access control is done for D2D. For a secure access control, existing techniques primarily used encryption, authentication and secret key sharing. However, the demand for 5G live implementation still needs a lot of effort and critical thinking.

C. Security Challenges Related to SDN/SDMN

1) Lessons Learned: SDN and SDMN are the current hot research topics for 5G communication security. Researchers still did not focus on the deep security schemes for SDN and SDMN. However, new breakthrough techniques are required in this area with the adoption of SDN and SDMN in the 5G communication networks.

Authors of [51] suggested the idea of developing a new mechanism to control state transition and storage inside the switch of a SDN data plane and implementation level verification methods for the security of inconsistency vulnerability. According to the authors of [161], SDN controller cluster will require a distributed security data storage scheme in future. Improvement in existing SDN and SDMN techniques are mandatory for achieving the target of future technology. Authors of [160] reflected various aspects of SDN security in detail including the improved security for ALL-ELEMENT threat model and the designing of modularized SDN regulators in the control domain.

2) Future Directions: Employing AI and ML approaches guarantee a softwarized security mechanisms to be deployed with 5G related technologies in conjunction with SDN such as NFV, MEC, and NS. Moreover, honeypots deployed with AI and ML platform can act as cyber defenders for deceiving the attackers in MEC systems. 5G networks are very likely to use multiple SDN controllers in the core. The efficient synchronization of security policies across multiple SDN controllers is needed to be addressed. Moreover, it is necessary to secure the communication between SDN controllers (East-West Interface) with proper security mechanism. Use of IPsec tunneling is one possibility to offer the required level of security for SDN East-West Interface.

D. MEC and Cloud Related Security Issues

1) Lessons Learned: MEC and cloud computing are the topics of high attention to many 5G researchers and scientists. Although lots of security solutions are available for cloud computing, not many security solutions are available for MEC. In 5G networks, the edge of the mobile network is the ingress access point to all the mobile network users and the services emanated in the RAN. This critical juncture is the weakest point of the entire network in terms of security. Core network elements have higher levels of security than the egde devices in both cyber and physical levels. Moreover, the security of the virtualized MEC platforms is still a gray area due to lesser deployments. Vulnerabilities and attacks plausible on Virtual Machines (VMs) are unique and cause significant consequences to the MEC system.

A number of authors provided security solutions for the network security. The efficient orchestration of existing diverse security mechanism is suggested by the authors of [197] that requires the universal view of available security solutions for the proper integration. Authors of [196] aimed to integrate block-chain technology in the proposed scheme. Authors of [194], aimed to further explore their proposed scheme of reputation-assisted optimization in DREAMS.

2) Future Directions: One of the most important security aspects related to MEC is to identify the treat vectors in a MEC systems. It is necessary to identify the vulnerability points in MEC systems and the nature of these threats associate with these vectors. Such a work can identify the possible existing security solutions that can be used to mitigate these attack.

Due to the dynamic nature of MEC based applications such as autonomous driving cars, industrial internet, AR/VR applications, a high level of AI/ML based solutions may be required for the provisioning of security at the edge devices in MEC. Moreover, big data analysis in MEC and cloud networks requires serious attention due to possibly high vulnerability and complexity of the system.

Moreover, osmotic computing [354] is a novel initiative introduced to achieve a seamless migration of edge and cloud computing infrastructures. The osmotic computing concept can be also utilize to deploy coherent security policies common to the edge and cloud data centres.

In addition, authors of [201], aimed to deploy ACPC for P2P storage cloud system and the design of particular scheduling schemes for trustworthy peers in a real-world scenario. For better trade-off authors of [204] aimed the possible data set combination in different dimensions. Authors of [199] targets to integrate conjunctive and disjunctive multi-keywords search in the proposed scheme as a future work for MEC systems.

E. Network Function Virtualization

1) Lessons Learned: Security in NFV has a significant impact on its adaptability in 5G network. Security will be largely impacting the system resiliency and the overall quality of the offered services in NFV based 5G network. Each NFVI component, i.e. NFV MANO, VNFs, VMs, hypervisors and physical hardware vulnerable to a different set of security challenges that pose threats to the whole NFVI. Therefore, different security mechanism should be used here. It is important to understand, NFVI is vulnerable to traditional cyber attacks, virtual element based attacks and physical attacks. Fig. 27 summarizes these generic security threats in NFV [355].

2) Future Directions: The security of NFV based 5G systems can be improved by using latest Machine Learning (ML) techniques. The existing policy-based security approaches used in NFV systems are tending to favor deductive reasoning by building models of reality and analyzing the models based on logical rules. However, the scalability of this system is limited due to complexity. This approach does not perform well in complex, dynamic and large systems such as 5G networks [3]. To mitigate this issue, an alternative way is to find truth from observation data and inductive reasoning. Recent past years, ML techniques have achieved rapid advancement in Big data handling domain. Novel ML based NFV Security services can be developed to improve the observation data and inductive reasoning. Thus, ML has potential to help NFV-based systems to better perform and protect. ML can enable autonomous operations of security mechanism in NFV systems. Within an abstracted and service API-oriented system, ML techniques can be used to analyze real-time data to fine-tune optimization parameters of the overall resource management scheme. Moreover, the ML system can adapt to load spikes (e.g., during a DDoS attack) with autonomous responses by learning from long-term operational data collected by human expert operators. Moreover, ML algorithms can be used for anomaly detection and learning latent structures or patterns from network activities. Thus, it can be used in discovery of invariants in functional, operational, causal and other relationships are crucial in many complex cyber-physical systems such as 5G networks.

Moreover, NFV can be used as a tool to improve the security of 5G networks. Specially, the added benefits of NFV such as flexibility and scalability can help to improve the incident response time, provides better resiliency against DDoS attacks. For instance, NFV can enables on-demand firewalling and IDS/ IPS to block or reroute malicious traffic. However the design of such dynamic NFV based security mechanism are yet to explored.

One of the critical issues in NFV is the tempering the VNF image. It is comparably easy to tamper the VNF images during migration to VMs. Within few seconds, it is possible to insert bugs such a malware into a VNF image file while it is being uploaded to an image database or being transferred from an image database to a compute node. In order to identify such tempering attempts, VNF images can be cryptographically signed and verified during launch time. This can be solved by setting up some signing authority and instruct the hypervisor to verify the signature of VNF image before the launch. Moreover, the remote attestation technique can be used to remotely verify the trust status of a NFV platform. The blockchain can be used as a technology to design such remote attestation systems.

Finally, Fig. 28 summarizes other security challenges in NFV [355] which are needed to be address in future 5G networks.

F. Network Slicing Related Security Issues

1) Lessons Learned: Network Slicing is rather a new technology in domain of network softwarization concepts. Most of the current research work were focusing on architectural and the implementation aspects of network slicing in 5G. Research focusing on solving the security issues related to slicing yet to be done.

2) Future Directions: Several security mechanisms must be implemented to achieve a secure network slicing system. However, these security mechanisms must be coordinated and securely communicate to ensure the reduce the security overhead and impact of security mechanism. To achieve this goal, allocation of an independent network slice for security is beneficial. For instance, security related communication such as authentication messages, firewall updates, security policy updates can be transported over this slice. In addition, network

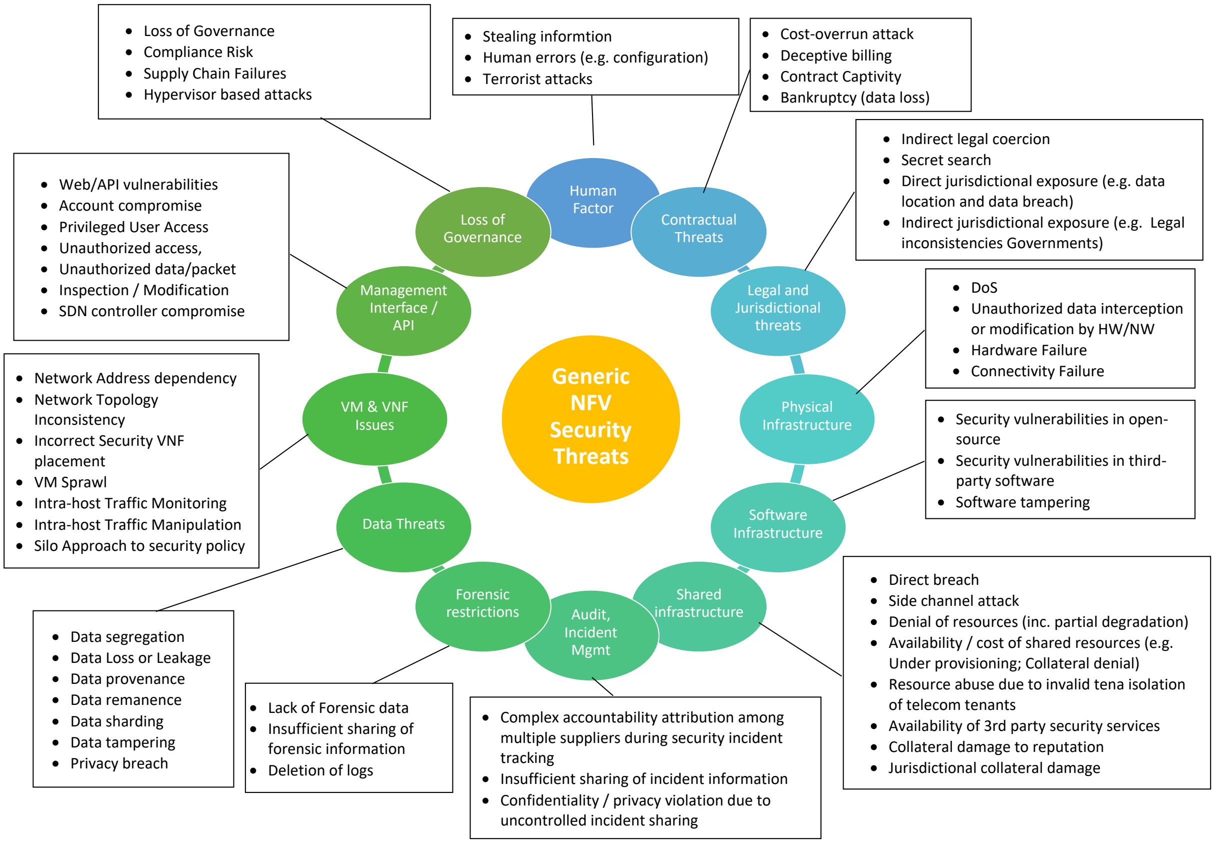

Generic NFV Security Threats
Loss of Governance
Compliance Risk
Supply Chain Failures
Hypervisor based attacks
Stealing informtion
Human errors (e.g. configuration)
Terrorist attacks
Cost-overrun attack
Deceptive billing
Contract Captivity
Bankruptcy (data loss)
Indirect legal coercion
Secret search
Direct jurisdictional exposure (e.g. data location and data breach)
Indirect jurisdictional exposure (e.g. Legal inconsistencies Governments)
Web/API vulnerabilities
Account compromise
Privileged User Access
Unauthorized access,
Unauthorized data/packet
Inspection / Modification
SDN controller compromise
DoS
Unauthorized data interception or modification by HW/NW
Hardware Failure
Connectivity Failure
Network Address dependency
Network Topology Inconsistency
Incorrect Security VNF placement
VM Sprawl
Intra-host Traffic Monitoring
Intra-host Traffic Manipulation
Silo Approach to security policy
Security vulnerabilities in open-source
Security vulnerabilities in third-party software
Software tampering
Direct breach
Side channel attack
Denial of resources (inc. partial degradation)
Availability / cost of shared resources (e.g. Under provisioning; Collateral denial)
Resource abuse due to invalid tena isolation of telecom tenants
Availability of 3rd party security services
Collateral damage to reputation
Jurisdictional collateral damage
Data segregation
Data Loss or Leakage
Data provenance
Data remanence
Data sharding
Data tampering
Privacy breach
Lack of Forensic data
Insufficient sharing of forensic information
Deletion of logs
Complex accountability attribution among multiple suppliers during security incident tracking
Insufficient sharing of incident information
Confidentiality / privacy violation due to uncontrolled incident sharing
Human Factor
Loss of Governance
Contractual Threats
Management Interface / API
Legal and Jurisdictional threats
VM & VNF Issues
Physical Infrastructure
Data Threats
Software Infrastructure
Forensic restrictions
Audit, Incident Mgmt
Shared infrastructure

Fig. 27. Generic Security Threats in NFV [355]

monitoring and security incident handling systems can be run on top of this security slice to make sure the proper operation of the network.

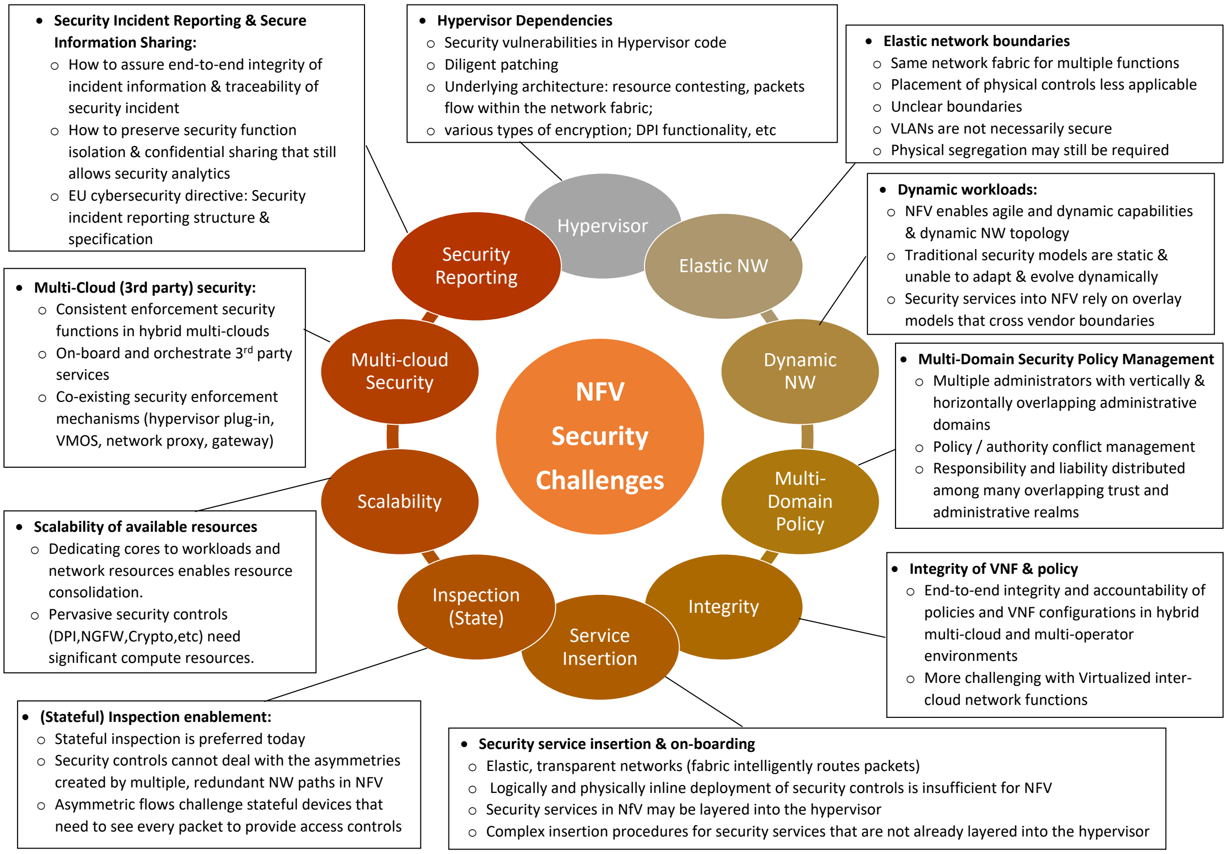
A dedicated security slice can ensure the end to end supply chain security of the systems. For instance, security related services such as security service management, SIEM, security monitoring, security service change management, cryptographic service, authentication and access control, security auditing and security service life cycle management can be implemented on top of this security slice. When a security slice is available, resources allocated for security services can be dynamically change. More importantly, it can ensure the availability of network resources for security.

In 5G networks, a network slice can be extended over multiple domains. As NS is used to set up, torn down or altered resources dynamically an on-demand basis, then the presence of orchestration is mandatory. To operate this function securely and smoothly, security policies have to be extended in to multiple domains. Thus, orchestrating security policies across multiple network domains also becomes important to ensuring the overall security of individual network slices.

G. Privacy

1) Lessons Learned: The 5G will likely be a fabric for the next generation of networks, for instances IoT, smart cities, industries, vehicles, etc. In such networks, an enormous quantity of data will be produced by the users, devices, applications, and machines. This (raw) data will be aggregated, stored, analyzed, processed, and fused for many different purposes including cross-borders. Moreover, this data not only belongs to an individual consumer but also to the citizens, societies, applications, verticals, organizations, and so on. In a typical network, the end-users' privacy risks emanate from the application data that will be communicated as plaintext in the network. Many of real data-leaks have proven that the end-users' privacy has been at high risks, and that data-leaks can be taken as the lessons from the past. Therefore, privacy has been one of the major issues in the 5G network.

2) Future Directions: As the 5G technologies are still at early stage, several future research directions can be explored in order to address the privacy issues. Specifically, it is possible to design 5G technologies that provide privacy protection from the origin of the data or embed privacy into each device, application, vertical, and service. The future research must focus on defining a general architecture for 5G privacy, including Privacy-by-Design (PbD). In addition, from the larger perspective of the 5G verticals, further topics can be explored, e.g., location privacy-based solutions for the MEC. In MEC, typically the data is processed at the edge devices and these devices are controlled and monitored by the operators. Privacy solutions may have direct impact on 5G applications such as IoT, healthcare, and smart cities, however, these solutions are still not adequately explored under the real world conditions.



- **Security Incident Reporting & Secure Information Sharing:**
  - How to assure end-to-end integrity of incident information & traceability of security incident
  - How to preserve security function isolation & confidential sharing that still allows security analytics
  - EU cybersecurity directive: Security incident reporting structure & specification

- **Hypervisor Dependencies**
  - Security vulnerabilities in Hypervisor code
  - Diligent patching
  - Underlying architecture: resource contesting, packets flow within the network fabric;
  - various types of encryption; DPI functionality, etc

- **Elastic network boundaries**
  - Same network fabric for multiple functions
  - Placement of physical controls less applicable
  - Unclear boundaries
  - VLANs are not necessarily secure
  - Physical segregation may still be required

- **Dynamic workloads:**
  - NFV enables agile and dynamic capabilities & dynamic NW topology
  - Traditional security models are static & unable to adapt & evolve dynamically
  - Security services into NFV rely on overlay models that cross vendor boundaries

- **Multi-Cloud (3rd party) security:**
  - Consistent enforcement security functions in hybrid multi-clouds
  - On-board and orchestrate 3rd party services
  - Co-existing security enforcement mechanisms (hypervisor plug-in, VMOS, network proxy, gateway)

- **Multi-Domain Security Policy Management**
  - Multiple administrators with vertically & horizontally overlapping administrative domains
  - Policy / authority conflict management
  - Responsibility and liability distributed among many overlapping trust and administrative realms

- **Scalability of available resources**
  - Dedicating cores to workloads and network resources enables resource consolidation.
  - Pervasive security controls (DPI,NGFW,Crypto,etc) need significant compute resources.

- **Integrity of VNF & policy**
  - End-to-end integrity and accountability of policies and VNF configurations in hybrid multi-cloud and multi-operator environments
  - More challenging with Virtualized inter-cloud network functions

- **(Stateful) Inspection enablement:**
  - Stateful inspection is preferred today
  - Security controls cannot deal with the asymmetries created by multiple, redundant NW paths in NFV
  - Asymmetric flows challenge stateful devices that need to see every packet to provide access controls

- **Security service insertion & on-boarding**
  - Elastic, transparent networks (fabric intelligently routes packets)
  - Logically and physically inline deployment of security controls is insufficient for NFV
  - Security services in NfV may be layered into the hypervisor
  - Complex insertion procedures for security services that are not already layered into the hypervisor

Fig. 28. Security Challenges in NFV [355]

Moreover, another approaches, for instance software defined privacy (SDP) based solutions can be extended into the 5G network [313]. The SDP-based solutions are based on privacy policies, which are defined by the privacy officers [356]. However, how to manage and store any data with various policy mechanisms are still under study.

5G has different stakeholders (such as a mobile network, ISP, CSP) and multiple verticals (such as healthcare, smart grid, transport and other critical infrastructure). All these entities may work collaboratively but may have different objectives. As a result, more efforts on the privacy regulations are highly required at different levels such as government, industry and consumer level.

H. Security Monitoring and Management

1) Lessons Learned: The main issue of current monitoring systems is the lack of visibility and controls on NFV based virtual network entities. Moreover the heterogeneity of different virtual entities makes many performance assessment applications ineffective. Therefore, it is important to study the impact of virtualization technologies such as SDN, NFV and cloud computing on existing monitoring systems. For instance, 5G network monitoring applications should be able to monitor and manage virtual entities.

2) Future Directions: One possibility to monitor these virtual entities is to monitor inter-VNF communication channel. However, it might not be possible to monitor inter-VNF communication under current specifications. Current OpenStack specifications provide blackprints to conduct the inter-VNF communication, however these specifications are not yet part of the current release [290].

Fig. 29 proposes how to extend the SDM architecture proposed in [290], [291], [294], [295] to use in 5G architecture. Here, we propose to add Software Defined Monitoring Controller (SDMC) as a NF in 5G core network. Virtual probes are deployed in every VNF in addition to the physical probes in physical hardware components.

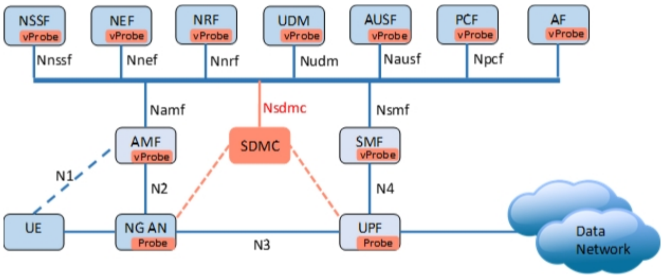


Fig. 29. New 5G Software Defined Monitoring (SDM) architecture.

The operational cost is another important aspect to consider in 5G monitoring system. The novel monitoring mechanisms and technologies need to cope with ever-changing contexts and trade-offs between the monitoring costs and the benefits involved.

On the other hand, current SDN based network topologies including 5G networks are no longer as static as they were when their implementation was only physical. These SDN networks allow a very dynamic configuration of routes, firewalls, filters and converters. It is also important to consider the backward compatibility for non-SDN based legacy mobile networks such as 4G-LTE. Thus is challenging to design 5G monitoring systems that can tackle the coexistence of legacy network components, software network components and virtualized network functions. The new 5G monitoring systems should be able to show a unified view of the network topology. To build such a unified view, it is required the Network Descriptor module which could collect and normalize network data from a wide range of sources as SDN controllers, networks emulators and legacy infrastructure. Moreover, it is also necessary to build a tool or a topology viewer which can represent the information has been collected from the network.

Moreover, significant improvements are needed in the following main areas to design an effective monitoring system in 5G networks. First, new **Information extraction** methods and techniques have to be designed to deal with virtualization. These methods able to obtain information on traffic flows, profiles, and properties by means of extracted protocol metadata, measurements, data mining and machine learning techniques. Second, the monitoring methods have to tackle the **scalability and performance issues.** Especially, the deployment of the 5G monitoring entities and the location of the observation points have to be carefully selected to assure the scalability. Moreover, monitoring tools should be selected to obtain the best balance between performance, cost and completeness of the monitoring outputs. Moreover, different hardware acceleration and packet pre-processing technologies can be integrated with the 5G monitoring systems to obtain highly optimized results. Thirdly, 5G monitoring system should support the **Heterogeneity.** The monitoring system should be able to analysis of different control and user plane traffic flows over the 5G network domains. It should also support the new interfaces between 5G entities and existing pre-5G networks entities. Fourthly, 5G monitoring systems should support **dynamicity.** Due to virtualized networks and applications in 5G network, 5G networks are highly dynamic. Changes in the network become quite easy and frequent in 5G network. Monitoring solutions need to be able to adapt to these changes to provide the proper operation.

I. Security Standardization

1) Lessons Learned: As of today, the functional nature of the 5G network for different stakeholders including consumers, industries and governments is underway. Through distinct working groups have been working on different topics and stakeholders in 5G security standards, yet no peculiar security standard for 5G network security is in use. Therefore, one take-away from such situation is that the *integration* and *cooperation* between different working groups, globally, are highly required to become reality for 5G network.

2) Future Directions: 5G security standards working groups, such as ITU, ETSI, 3GPP, oneM2M, 5G PPP, IEEE, IETF, NVF, ONF, are working on a large number of security issues. These groups are developing security recommendations, technical specifications, defining security architecture and principles, M2M security specifications, identifying security risks, etc. It is a promising initiative, but more precise 5G standards and security mechanisms (authentication, confidentiality, integrity, availability) are required to build such a mammoth scale 5G network. It is clear that more efforts are required to develop a large number of standards to make the 5G function efficiently and securely.

J. PHY Layer Security

1) Lessons Learned: For the current literature review, noticeably several researchers have done a lot of research for PLS. A number of algorithms exists for high security provision. Most of the latest work used AN for better security of the system. Table IX shows a list of goals and achievements made by several authors in multiple ways. The newly implemented technique somehow opposes cryptography in PLS. It is also noticeable that physical layer is the most vulnerable layer for 5G technology. Since the entire world will face a new type of technology in terms of, smart or connected world. Hence, there is high amount of security threat to more connected devices. Internet of everything will bring connectivity for everything. Hence, every thing will face some security threats.

2) Future Directions: For the physical layer security of NOMA, OFDMA, MIMO, UAV, D2D and mmWave most of the authors worked on PLS without cryptography. However, for achieving challenging 5G security targets joint consideration of cryptography design and key assisted physical layer security will provide best security scheme. Better implementation of AS and jammers is necessary for achievement of QoS. Implementation of AI security or machine learning technique will definitely improve the system security. Authors in [357] combined M-NOMA with genetic algorithm. It will be helpful for better system security.

Security in UAVs and mmWave still has not received the significant attention of many researchers. Most of the security research is done in terms of threat detection, response to intruders reaction, maximization of secrecy rate and cryptography. There are many already proposed secure network scheme, used for other Physical layer technologies, which can be implemented on UAVs and mmWave. Further, practical implementation of many techniques requires consideration. FPGA implementation is a better tool for the proof of theoretical work.

According to [211], For different variation including the block size and the activation ratio, the proposed OFDM-SIS scheme's secrecy performance requires investigation and Overall system achievement including secrecy and other dominant functionalities can be maximized by exploiting the degree of freedom given by the proposed OFDM-SIS scheme. In [52], security techniques for overall QoS, limitations of 5G, cross-layer, and content aware PLS are considered as some of the future directions. In future authors of cite he2017design intent to extend the technique to MIMO secure NOMA, prevent the privacy amongst user due to SICs performed at each user, and to code domain NOMA. According to the authors of [236], optimization of power allocation coefficients could be a future work for CR NOMA security.

According to the authors of [220], exploring the system under robust allocations of resources under uncertainty channel models is one of the future work. In addition, the system can utilize multiple antennas for the better performance of the system.

It would be of interest to study the deployment of PHY security in industrial control systems, merging modest cryptographic approaches with PHY-layer methods can augment general security and economical. PHY-layer authentication is an indispensable way for averting Probing-free spoofing attack in the industrial control systems – this helps to guarantee that only the legitimate signals are decoded [358]. Thus, deploying PHY layer techniques and tailoring them for industrial control system stands as a new research avenue. In recent literature [359], [360] resort to machine learning techniques to improve channel state information based authentication. This is indeed a new research direction to use artificial intelligent to improve the PHY layer security schemes.

Industry 4.0 entails the current inclination of automation and data exchange in industrial technologies; cyber-physical systems, the Internet of things, cloud computing and intelligent computing [361]. Integration of PHY layer security with Industry 4.0 opens up a new horizon for wireless PHY research community.

K. SDN-NFV Security

1) Lessons Learned: 5G networks are fundamentally based on SDN and NFV. On one hand, SDN/NFV could solve the most of the security limitations in 4G-LTE networks. On the other hand, most of the SDN/NFV security challenges are also applicable to 5G networks. Thus, 5G networks will have additional security requirements, such as SDN controller security, hypervisor security, orchestrator security, cloud security as well as security under multi-tenancy settings. Software errors such as misconfigurations of VNFs can lead to inter-federated conflicts that can jeopardize the whole network. In addition to security challenges and opportunities associated with SDN/NFV networks, 5G networks tackle the security challenges in the various section of the network. For instance, RAN should include additional security measures to prevent DDoS via smart phones, resource exhaustion attacks and misuse infrastructure sharing. Moreover, authentication schemes such as EAP should be modified not only to support URLLC applications with less than 1 ms delay, but also authenticate millions of connected devices (i.e IoT) simultaneously.

2) Future Directions: One possible solution is to mitigate the quickly identify security treats or attacks on 5G networks and try to limit the impacts those attacks have on customers and other core network elements. NFV offers better monitoring features such as distribute monitoring functions than SDN. On the other hand, SDN offers flexibility to divert traffic flows at switch level. Thus combine use of these features can be used to quickly identify and limit or block malicious traffic flows much closer to the source of attacks. Due the tremendous increment in data traffic volume and subscribers, it is necessary to design automated solutions by using novel AI/ML techniques. Moreover, new interfaces and shared databases should be established between SDN and NFV platforms to enable the cooperation.

L. Key Management and Secure Communication

1) Lessons Learned: Secure communication between different control entities is required to operate reliable and efficient mobile network. The efficient integration of key management entities with 5G core network elements is necessary to enable such secure communication in 5G. Moreover, current secure communication systems need frequent key exchanges and security parameter updates with these core security elements. However, the security maintenance overhead (i.e. bandwidth, battery life, processing power, communication cost) is increasing in 5G due to increment of control entities (e.g. number of BSs, core network elements and subscribers). Thus, future secure communication systems should be more efficient than current systems to mitigate this challenge.

2) Future Directions: In that aspects, Quantum security can be the one of the evolutionary tide of network security and cryptography areas. When the adversaries become unconquerable with the quantum level powers, the existing public-key encryption and signature schemes will no longer provide secure connectivity. The security of quantum cryptography can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper. Longer symmetric keys derived and distributed by quantum cryptographic approaches will ensure the lifetime security of many IoT devices. This will also extend the battery life of the devices and minimize the network overhead by reducing frequent handshaking for the key establishment process. Furthermore, the quantum security can be exploited for managing secure identity, mutual authentication of the devices, appropriate certification and qualification, and power efficient algorithms and policies.

In addition, some of the key management entities can be implemented at the edge of the network by utilizing MEC capabilities. This can reduce the security related communication overhead over 5G backhual network. This approach will be paving the way for the delay critical IoT and 5G applications as well.

M. Other related/future technologies to enhance security and privacy in 5G

1) Context-Aware Security: With the development of ubiquitous computing, it is expected that context aware communication and networking will dominate in beyond 5G era. Many of the future apps need reliable access to various sources of context information. For instance, precise location information on both indoors and outdoors will be required to offer multimedia delivery every time and everywhere, rapid file sharing in the form of cellular broadcasting and wireless car video services. Future mobile communication networks (beyond 5G) are also very frequently integrated with IoT/IoE

(Internet of Everything) networks to provide wide range of novel services. Thus, at one end, these heterogeneous kinds of networks will be considered crucial for improving context awareness but on the other end, security and privacy risks will also emerge. Adversaries can target such networks more easily to launch various security attacks. Also as users are naturally interested in protecting their privacy and thus only the required information shall be collected for the purposes of context-aware operation. Therefore, context awareness based security mechanism requires intelligent and controlled solutions by the network operator and other involved stockholders.

2) AI for Security: The existing security mechanisms for mobile networks are either human or machine-centric. The human centric systems rely on the manual configuration of humans and machine on centric systems rely automated techniques such as anomaly detection. However, such system still makes fault negativity which might need human intervention at the end to fix those issues. Moreover, future digital systems will face more automated and advance attacks (e.g. AI-enabled hacking) due the advancement of communication technology and machine learning techniques. To prevent such attacks, 5G need sophisticated and intelligent security solutions. Ironically, AI is the best hope to combat against these attacks. The development in AI, i.e. cognitive algorithms motivate us to use AI for fulfilling the stringent delay and extremely sensitive security requirements. AI machines intelligently select data, transform it into meaningful information and then make decisions of controlling processes. Even further, AI algorithms and models such as Markov models, neural networks, genetic algorithms, and machine learning techniques can be used to find configuration errors, security vulnerabilities and threats.

However, machine learning, fuzzy logic and other techniques related to AI are not sufficient enough to tackle several advance 5G technology communication technique specially IoT and Big Data. Therefore, AI techniques needs to be upgraded in a more sophisticated and acceptable manner to provide high levels of security to fulfill the required expectations.

3) Security Orchestration and Automation: The use of security orchestration is mandatory 5G networks where the operator needs to control both virtual and physical network segments. The primary goal of security orchestration is remove the need for manually configure with human interaction. Human central security management is no longer feasible due to high dynamicity of the future mobile network. The security orchestrator will be responsible for deployment, configuration, maintenance, monitoring and life cycle management all security functions in a softwarized 5G mobile network. It should be able to ensure the end-to-end security by automatically aligning the security policies inside the both virtual and physical network segments. ETSI ISG group has already defined the security orchestrator for NFV systems. The group has also defined different tasks of the security orchestrator in NFV systems and the required interfaces to interact with the existing ETSI NFV components such as NFV orchestrator, the VNF Managers, the Element Managers and the Virtual Infrastructure Managers. Since, several other network softwarization techniques such as SDN, MEC and NS will also be a part of the 5G network and the functions of security orchestration should be extended to manage the security of other systems as well. The integrated role of security orchestrator in 5G systems should be defined along with the new interfaces to communicate with different 5G technologies.

4) Blockchain: For some researchers and industry, the blockchain technology is considering as one of the most important innovations in this century. It might be true since a recent market study estimates blockchain will add 3.1 trillion Euro in business value by 2030 [362]. Blockchain has already adopted in one of major 5G domain which is IoT.

Due the popularity of the IoT systems, billions of smart devices will be connected by 5G network. This will raise serious concerns on security, privacy, connectivity, service provisioning and data storage ares. Most of the present day IoT systems are using centralized cloud based architecture. A centralized cloud is used for data processing as well as storage. However, the current centralized cloud architecture will be difficult to scale up to satisfy the demands of future 5G IoT systems. To solve this issues, the decentralized and consensus-driven Blockchain has identified as a viable solution. Blockchain can play a significant role in IoT domain [363]–[365]. Blockchain can be used to enable secure data sharing, secure authentication and high privacy in 5G IoT Systems.

On the other hand, several analysis has estimated that global IoT market is expected to grow up to 457 billion Euro by 2020. The combination of IoT and Blockchain will disrupt existing processes across variety of industries including manufacturing, agriculture, banking, transportation, shipping, energy, the financial sector and healthcare. However, it is still in its infancy. Moreover, the combination with IoT still requires essential insights with respect to concrete application domains, performance, scalability, security and privacy issues. In this regard, the use of smart contracts will help to design more dynamic and self-executing security policies. Specifically, researchers should be targeting of designing blockchain based mechanisms to support identity management, access control systems, anonymity and privacy, and trust models.

In addition, blockchain can be used in cloud computing systems to enable security, privacy and automation [366]–[369]. Since 5G is promoting novel MEC based solutions which is proposing to move cloud computing features to the edge, blockchain will be important in MEC domain as well. Specially, blockchain can fuel the integration of MEC IoT integration in 5G by offering a high level of security and privacy. Some research work related to blockchain based Fog computing systems were proposed to improve the security and privacy [370]–[375]. Thus, blockchain can play a vital role in enhancing security of not only MEC but also other 5G technologies such as SDN, NFV and network slicing.

In addition, blockchain can be used to enhance the security of 5G network by mitigating roaming frauds. A roaming fraud occurs when a fake mobile subscriber accesses the resources of the home network via the visitor network. In this case, the home network operator is unable to charge the subscriber for the services provided. However, he is is obliged to pay the visitor network for the roaming services. Most of the roaming fraud exploits due to long detection time and long response time due data transfer via third party data clearing houses. A blockchain could be implemented between every pair of operators which have a roaming agreement to speed up the detection and response times by eliminating third party data clearing houses. Moreover, blockchain can be used to offer identity-as-a-service to 5G verticals such as smart grids, health and other critical infrastructures. However, these areas are yet to be explored.

5) Security-by-Design (SbD): SbD is an approach that will consider the security concerns already at the beginning of a design a product, service or software. SbD can secure the foundation of the product or service by minimizing impact anticipated security vulnerabilities. Many software systems i.e Amazon Web Services (AWS) is using SbD to automates security controls and streamlines auditing. In current software systems, the current SbD approaches can offer benefits such as establishment reliable operation of controls and enabling continuous and real-time auditing. However, the core concept SbD is not limited to software systems. It can be extended to any system including 5G mobile networks. For instance, SbD approach can be along with NFV, SDN, MEC and NS systems. In this way, SbD approach can reduce the impact of know attacks on the system.

6) Security-as-a-Service: 5G networks provide services for a large variety of verticals including smart grids, transportation, health care, smart city, and future factories. However, most of these vertical operators will not have up-to-date security expertise to manage all security aspects of their network. Therefore, they must obtain a wide range of security services by security service providers. In this content, Security-as-a-Service (SaaS) is an approach where service providers can offer security services to cooperate customers.Typically, these security services are ranging from authentication, security monitoring intrusion detection, penetration testing and security event management, among others. As typical vertical operators do not have expertise in both network security and network softwarization, SaaS concept can offer easy integration route for them. This is an interesting research domain that has possibility to provide network security as a SaaS solution.

XI. Conclusion

The landscape of 5G network is continuously evolving, raising an increasing number of security threats at different levels and applications. This paper has explored 5G security threat via panoramic reviews and discussions based on available literature and have tried to provide a relevant understanding on the security issues. We have explored the comprehensive investigation on 5G security model, next generation threat landscape for 5G, IoT threat landscapes, and threat analysis in 5G networks. Our survey covered a holistic investigations on security challenges in key 5G security domains, including authentication, access control, communication security and encryption. The survey had also highlighted the identified security issues associated with 5G key technologies i.e. Software Defined Networking (SDN), Network Function Virtualization (NFV), cloud computing, Multi-access Edge Computing (MEC) and Network Slicing (NS) concepts. Then, the survey included a horizontal analysis of security monitoring and privacy aspects on 5G network. Finally, a comprehensive list of future directions and open challenges had included to encourage future research on 5G security domain.

Acknowledgment

This work is funded, in part, by the framework of Competitiveness Enhancement Program of the National Research Tomsk Polytechnic University No. TPU CEP IC 110/2017, in part, by the European Union under the RESPONSE 5G (Grant No: 789658) project.

References

[1] M. Agiwal, A. Roy, and N. Saxena, “Next Generation 5G Wireless Networks: A Comprehensive Survey,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[2] P. Zhang, X. Yang, J. Chen, and Y. Huang, “A Survey of Testing for 5G: Solutions, Opportunities, and Challenges,” *China Communications*, vol. 16, no. 1, pp. 69–85, 2019.

[3] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A Comprehensive Guide to 5G Security*. Wiley Publishing, 2018.

[4] G. Maier and M. Reisslein, “Transport SDN at the Dawn of the 5G Era,” 2019.

[5] M. S. Bonfim, K. L. Dias, and S. F. Fernandes, “Integrated NFV/SDN Architectures: A Systematic Literature Review,” *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, p. 114, 2019.

[6] S. Kitanov, B. Popovski, and T. Janevski, “Quality Evaluation of Cloud and Fog Computing Services in 5G Networks,” in *Enabling Technologies and Architectures for Next-Generation Networking Capabilities*. IGI Global, 2019, pp. 1–36.

[7] B. Han, S. Wong, C. Mannweiler, M. R. Crippa, and H. D. Schotten, “Context-Awareness Enhances 5G Multi-Access Edge Computing Reliability,” *IEEE Access*, vol. 7, pp. 21 290–21 299, 2019.

[8] S. Zhang, “An Overview of Network Slicing for 5G,” *IEEE Wireless Communications*, 2019.

[9] S. Sarraf, “5G Emerging Technology and Affected Industries: Quick Survey,” *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, vol. 55, no. 1, pp. 75–82, 2019.

[10] S. Li, L. Da Xu, and S. Zhao, “5G Internet of Things: A Survey,” *Journal of Industrial Information Integration*, 2018.

[11] R. Ahmed, A. K. Malviya, M. J. Kaur, and V. P. Mishra, “Comprehensive Survey of Key Technologies Enabling 5G-IoT,” *Available at SSRN 3351007*, 2019.

[12] S.-Y. Lien, C.-C. Tseng, I. Moerman, and L. Badia, “Recent Advances in 5G Technologies: New Radio Access and Networking,” *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[13] D. N. K. Jayakody, K. Srinivasan, and V. Sharma, *5G Enabled Secure Wireless Networks*. Springer, 2019.

[14] N. Nikaein, M. K. Marina, S. Manickam, A. Dawson, R. Knopp, and C. Bonnet, “Openairinterface: A flexible platform for 5g research,” *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 33–38, 2014.

[15] R. P. Jover, “The current state of affairs in 5g security and the main remaining security challenges,” *arXiv preprint arXiv:1904.08394*, 2019.

[16] A. Gupta and R. K. Jha, “A Survey of 5G Network: Architecture and Emerging Technologies,” *IEEE access*, vol. 3, pp. 1206–1232, 2015.

[17] A. Gohil, H. Modi, and S. K. Patel, “5G Technology of Mobile Communication: A Survey,” in *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on*. IEEE, 2013, pp. 288–292.

[18] N. Panwar, S. Sharma, and A. K. Singh, “A Survey on 5G: The Next Generation of Mobile Communication,” *Physical Communication*, vol. 18, pp. 64–84, 2016.

[19] M. Jaber, M. A. Imran, R. Tafazolli, and A. Tukmanov, “5G Backhaul Challenges and Emerging Research Directions: A Survey,” *IEEE access*, vol. 4, pp. 1743–1766, 2016.

[20] R. N. Mitra and D. P. Agrawal, “5G Mobile Technology: A Survey,” *ICT Express*, vol. 1, no. 3, pp. 132–137, 2015.

[21] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, “5G Security: Analysis of Threats and Solutions,” in *Standards for Communications and Networking (CSCN), 2017 IEEE Conference on*. IEEE, 2017, pp. 193–199.

[22] ——, "Overview of 5G Security Challenges and Solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[23] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G Cellular networks: A Survey of Existing Authentication and Privacy-Preserving Schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018.

[24] G. Mantas, N. Komninos, J. Rodriuez, E. Logota, and H. Marques, *Security for 5G Communications*. John Wiley & Sons, Ltd., 2015.

[25] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-Defined Mobile Networks Security," *Mobile Networks and Applications*, vol. 21, no. 5, pp. 729–743, 2016.

[26] P. Gandotra and R. K. Jha, "A survey on green communication and security challenges in 5G wireless communication networks," *Journal of Network and Computer Applications*, vol. 96, pp. 39–61, 2017.

[27] A. K. Rangisetti and B. R. Tamma, "Software Defined Wireless Networks: A Survey of Issues and Solutions," *Wireless Personal Communications*, vol. 97, no. 4, pp. 6019–6053, 2017.

[28] A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck, "Software Defined Networking for Security Enhancement in Wireless Mobile Networks," *Computer Networks*, vol. 66, pp. 94–101, 2014.

[29] G. Choudhary and V. Sharma, "A Survey on the Security and the Evolution of Osmotic and Catalytic Computing for 5G Networks," in *5G Enabled Secure Wireless Networks*. Springer, 2019, pp. 69–102.

[30] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and C. Pöpper, "On Security Research towards Future Mobile Network Generations," *IEEE Communications Surveys & Tutorials*, 2018.

[31] W. Li, W. Meng, and L. F. Kwok, "A Survey On OpenFlow-Based Software Defined Networks: Security Challenges and Countermeasures," *Journal of Network and Computer Applications*, vol. 68, pp. 126–139, 2016.

[32] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security In Software Defined Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2317–2346, 2015.

[33] I. Alsmadi and D. Xu, "Security of Software Defined Networks: A Survey," *computers & security*, vol. 53, pp. 79–108, 2015.

[34] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[35] W. Yang and C. Fung, "A Survey On Security In Network Functions Virtualization," in *NetSoft Conference and Workshops (NetSoft), 2016 IEEE*. IEEE, 2016, pp. 15–19.

[36] H. Jang, J. Jeong, H. Kim, and J.-S. Park, "A Survey on Interfaces to Network Security Functions in Network Virtualization," in *Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on*. IEEE, 2015, pp. 160–163.

[37] I. Farris, T. Taleb, Y. Khettab, and J. S. Song, "A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems," *IEEE Communications Surveys & Tutorials*, 2018.

[38] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A Survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[39] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[40] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[41] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[42] W. H. Hassan *et al.*, "Current Research on Internet of Things (IoT) Security: A Survey," *Computer Networks*, vol. 148, pp. 283–294, 2019.

[43] D. Mewada, N. Dave, and R. K. Prajapati, "A Survey: Prospects of Internet of Things (IoT) Using Cryptography Based on its Subsequent Challenges," *Australian Journal of Wireless Technologies, Mobility and Security e-ISSN 2200-1883*, vol. 1, no. 1, pp. 28–30, 2019.

[44] V. Sharma, I. You, K. Andersson, F. Palmieri, and M. H. Rehmani, "Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey," *arXiv preprint arXiv:1903.05362*, 2019.

[45] J.-Y. Yu and Y.-G. Kim, "Analysis of IoT Platform Security: A Survey," in *2019 International Conference on Platform Technology and Service (PlatCon)*. IEEE, 2019, pp. 1–5.

[46] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *arXiv preprint arXiv:1904.05735*, 2019.

[47] N. Tariq, M. Asim, F. Al-Obeidat, M. Zubair Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, "The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey," *Sensors*, vol. 19, no. 8, p. 1788, 2019.

[48] N. Gray, S. Lange, T. Zinner, B. Pfaff, and D. Hock, "Evaluation of a Distributed Control Plane for Managing Heterogeneous SDN-enabled and Legacy Networks," in *2018 IEEE Seventh International Conference on Communications and Electronics (ICCE)*. IEEE, 2018, pp. 361–366.

[49] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[50] R. Tourani, T. Mick, S. Misra, and G. Panwar, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," *arXiv preprint arXiv:1603.03409*, 2016.

[51] T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, and M. Conti, "A Survey on the Security of Stateful SDN Data Planes," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1701–1725, 2017.

[52] L. Sun and Q. Du, "Physical Layer Security With Its Applications In 5G Networks: A Review," *China Communications*, vol. 14, no. 12, pp. 1–14, 2017.

[53] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[54] P. Singh, P. Pawar, and A. Trivedi, "Physical Layer Security Approaches in 5G Wireless Communication Networks," in *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*. IEEE, 2019, pp. 477–482.

[55] O. N. Hamoud, T. Kenaza, and Y. Challal, "Security In Device-To-Device Communications: A Survey," *IET Networks*, vol. 7, no. 1, pp. 14–22, 2017.

[56] Z. Shaokun, Z. Lei, M. Juntao, Y. Xinlei, and M. Nan, "Security Analysis of Control Plane in ASON," in *Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012 Second International Conference on*. IEEE, 2012, pp. 623–626.

[57] M. Liyanage, A. Gurtov, and M. Ylianttila, *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*. John Wiley & Sons, 2015.

[58] P. Lapsley, "The History of Phone Phreaking," *Exploding the Phone*, pp. 2005–2009, 2011.

[59] M. I. Baba, N. Nafees, I. Manzoor, K. A. Naik, and S. Ahmed, "Evolution of Mobile Wireless Communication Systems from 1G to 5G: A Comparative Analysis," 2018.

[60] S. Yadav and S. Singh, "Review Paper on Development of Mobile Wireless Technologies (1G to 5G)," *International Journal of Computer Science and Mobile Computing*, 2018.

[61] T. S. Rappaport *et al.*, *Wireless Communications: Principles and Practice*. prentice hall PTR New Jersey, 1996, vol. 2.

[62] C. Hanser, S. Moritz, F. Zaloshnja, and Q. Zhang, "Security in Mobile Telephony: The Security Levels in the Different Handy Generations," *Uppsala Universitet, Uppsala*, 2014.

[63] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[64] S. Patel, V. Shah, and M. Kansara, "Comparative Study of 2G, 3G and 4G," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2018.

[65] Y. E. H. El Idrissi, N. Zahid, and M. Jedra, "Security Analysis of 3GPP (LTE)WLAN Interworking and a New local Authentication Method Based on EAP-AKA," in *The First International Conference on Future Generation Communication Technologies*. IEEE, 2012, pp. 137–142.

[66] M. Liyanage and A. Gurtov, "Secured VPN Models for LTE Backhaul Networks," in *2012 IEEE Vehicular Technology Conference (VTC Fall)*. IEEE, 2012, pp. 1–5.

[67] M. Liyanage, M. Ylianttila, and A. Gurtov, "A Case Study on Security Issues in LTE Backhaul and Core Networks," *Case Studies in Secure Computing: Achievements and Trends*, vol. 1, p. 167, 2014.

[68] S. K. Mohapatra, B. R. Swain, and P. Das, "Comprehensive Survey of Possible Security Issues on 4G Networks," *International Journal of Network Security & Its Applications*, vol. 7, no. 2, p. 61, 2015.

[69] M. Liyanage, M. Ylianttila, and A. Gurtov, “IP-Based Virtual Private Network Implementations In Future Cellular Networks,” in *Handbook of Research on Progressive Trends in Wireless Communications and Networking*. IGI Global, 2014, pp. 44–66.

[70] S. E. Elayoubi, M. Fallgren, P. Spapis, G. Zimmermann, D. Martín-Sacristán, C. Yang, S. Jeux, P. Agyapong, L. Campoy, Y. Qi *et al.*, “5G Service Requirements and Operational Use Cases: Analysis and METIS II Vision,” in *Networks and Communications (EuCNC), 2016 European Conference on*. IEEE, 2016, pp. 158–162.

[71] S. Gold, “The Rebirth of Phreaking,” *Network security*, vol. 2011, no. 6, pp. 15–17, 2011.

[72] M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, “Secure Communication Channel Architecture for Software Defined Mobile Networks,” *Computer Networks*, vol. 114, pp. 32–50, 2017.

[73] X. Zhang, A. Kunz, and S. Schröder, “Overview of 5g security in 3gpp,” in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2017, pp. 181–186.

[74] M. H. Eiza, Q. Ni, and Q. Shi, “Secure and privacy-aware cloud-assisted video reporting service in 5g-enabled vehicular networks,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 7868–7881, 2016.

[75] Z. Chen, F. Zhang, P. Zhang, J. K. Liu, J. Huang, H. Zhao, and J. Shen, “Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control,” *Future Generation Computer Systems*, vol. 87, pp. 712–724, 2018.

[76] J. Pacheco, D. Ibarra, A. Vijay, and S. Hariri, “IoT Security Framework for Smart Water System,” in *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*. IEEE, 2017, pp. 1285–1292.

[77] S.-R. Oh and Y.-G. Kim, “Development of IoT Security Component for Interoperability,” in *Computer Engineering Conference (ICENCO), 2017 13th International*. IEEE, 2017, pp. 41–44.

[78] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. Leung, “Secure Resource Allocation for OFDMA Two-Way Relay Wireless Sensor Networks Without and With Cooperative Jamming,” *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1714–1725, 2016.

[79] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, “Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications,” *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[80] C. Li, Z. Qin, E. Novak, and Q. Li, “Securing SDN Infrastructure of IoT–Fog Networks From MitM Attacks,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1156–1164, 2017.

[81] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, “Malware Threats and Detection for Industrial Mobile-IoT Networks,” *IEEE access*, vol. 6, pp. 15 941–15 957, 2018.

[82] S. Choi, J. Song, J. Kim, S. Lim, S. Choi, T. T. Kwon, and S. Bahk, “5G K-SimNet: End-to-End Performance Evaluation of 5G Cellular Systems,” in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2019, pp. 1–6.

[83] S. Gupta, B. L. Parne, and N. S. Chaudhari, “Security Vulnerabilities in Handover Authentication Mechanism of 5G Network,” in *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*. IEEE, 2019, pp. 369–374.

[84] L. M. Larsen, M. S. Berger, and H. L. Christiansen, “Fronthaul for cloud-ran enabling network slicing in 5g mobile networks,” *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[85] T. Q. Thanh, S. Covaci, and T. Magedanz, “Viseco: An annotated security management framework for 5g,” in *International Conference on Mobile, Secure, and Programmable Networking*. Springer, 2018, pp. 251–269.

[86] F. Al-Turjman, “5G-Enabled Devices and Smart-Spaces in Social-IoT: An Overview,” *Future Generation Computer Systems*, vol. 92, pp. 732–744, 2019.

[87] M. Agiwal, N. Saxena, and A. Roy, “Towards Connected Living: 5G enabled Internet of Things (IoT),” *IETE Technical Review*, vol. 36, no. 2, pp. 190–202, 2019.

[88] F. Jameel, M. A. Javed, D. N. Jayakody, and S. A. Hassan, “On Secrecy Performance of Industrial Internet of Things,” *Internet Technology Letters*, vol. 1, no. 2, p. e32, 2018.

[89] F. Pan, Z. Pang, M. Luvisotto, M. Xiao, and H. Wen, “Physical-layer security for industrial wireless control systems: Basics and future directions,” *IEEE Industrial Electronics Magazine*, vol. 12, no. 4, pp. 18–27, 2018.

[90] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, “Evaluating Critical Security Issues of The IoT World: Present and Future Challenges,” *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[91] M. Yasin, T. Tekeste, H. Saleh, B. Mohammad, O. Sinanoglu, and M. Ismail, “Ultra-Low Power, Secure IoT Platform for Predicting Cardiovascular Diseases,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 9, pp. 2624–2637, 2017.

[92] U. Mbanaso and G. Chukwudebe, “Requirement Analysis of IoT Security in Distributed Systems,” in *Electro-Technology for National Development (NIGERCON), 2017 IEEE 3rd International Conference on*. IEEE, 2017, pp. 777–781.

[93] S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. Mahapatra, “Security Enhancements to System on Chip Devices for IoT Perception Layer,” in *Nanoelectronic and Information Systems (iNIS), 2017 IEEE International Symposium on*. IEEE, 2017, pp. 151–156.

[94] Y. Zhang, L. Xu, Q. Dong, J. Wang, D. Blaauw, and D. Sylvester, “Recryptor: A Reconfigurable Cryptographic Cortex-M0 Processor With In-Memory and Near-Memory Computing for IoT Security,” *IEEE Journal of Solid-State Circuits*, 2018.

[95] J. Wang, R. Zhu, and S. Liu, “A Differentially Private Unscented Kalman Filter for Streaming Data in IoT,” *IEEE Access*, vol. 6, pp. 6487–6495, 2018.

[96] N. Alliance, “5G Security Recommendations Package,” *White paper*, 2016.

[97] ——, “5G Security Recommendations Package 1,” 2016.

[98] ——, “5G Security Recommendations Package 2: Network Slicing,” 2016.

[99] ——, “5G security–Package 3: Mobile Edge Computing/Low Latency/Consistent User Experience,” 2016.

[100] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, “A Formal Analysis of 5G Authentication,” in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 1383–1396.

[101] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, “Insecure connection bootstrapping in cellular networks: the root of all evil,” in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2019, pp. 1–11.

[102] C. Cremers and M. Dehnel-Wild, “Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion,” in *Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2019.

[103] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, “New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols,” 2019.

[104] S. Behrad, E. Bertin, and N. Crespi, “Securing Authentication for Mobile Networks, A Survey on 4G Issues and 5G Answers,” in *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 2018, pp. 1–8.

[105] J. Arkko, K. Norrman, M. Näslund, and B. Sahlin, “A USIM Compatible 5G AKA Protocol with Perfect Forward Secrecy,” in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, vol. 1. IEEE, 2015, pp. 1205–1209.

[106] R. Giustolisi and C. Gerhmann, “Threats To 5G Group-Based Authentication,” in *13th International Conference on Security and Cryptography (SECRYPT 2016), 26-28 July 2016, Madrid, Spain*. SciTePress, 2016.

[107] A. Koutsos, “The 5G-AKA Authentication Protocol Privacy,” *arXiv preprint arXiv:1811.06922*, 2018.

[108] A. Braeken, M. Liyanage, P. Kumar, and J. Murphy, “Novel 5g authentication protocol to improve the resistance against active attacks and malicious serving networks,” *IEEE Access*, pp. 1–1, 2019.

[109] A. Ozhelvaci and M. Ma, “Secure and efficient vertical handover authentication for 5g hetnets,” in *2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP)*. IEEE, 2018, pp. 27–32.

[110] T. Ma and F. Hu, “A cross-layer collaborative handover authentication approach for 5g heterogeneous network,” in *Journal of Physics: Conference Series*, vol. 1169, no. 1. IOP Publishing, 2019, p. 012066.

[111] S. B. M. Baskaran, G. Raja, A. K. Bashir, and M. Murata, “QoS-Aware Frequency-Based 4G+ Relative Authentication Model for Next Generation LTE and Its Dependent Public Safety Networks,” *IEEE Access*, 2017.

[112] M. Wang and Z. Yan, “Privacy-Preserving Authentication and Key Agreement Protocols for D2D Group Communications,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3637–3647, 2018.

[113] S. Shin and T. Kwon, “Two-Factor Authenticated Key Agreement Supporting Unlinkability in 5G-Integrated Wireless Sensor Networks,” *IEEE ACCESS*, vol. 6, pp. 11 229–11 241, 2018.

[114] M. G. Pérez, A. H. Celdrán, F. Ippoliti, P. G. Giardina, G. Bernini, R. M. Alaez, E. Chirivella-Perez, F. J. G. Clemente, G. M. Pérez, E. Kraja *et al.*, “Dynamic Reconfiguration in 5G mobile Networks to Proactively Detect and Mitigate Botnets,” *IEEE Internet Computing*, vol. 21, no. 5, pp. 28–36, 2017.

[115] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[116] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-Preserving Schemes," *Journal of Network and Computer Applications*, 2017.

[117] G. Chopra, R. K. Jha, and S. Jain, "A Survey on Ultra-Dense Network and Emerging Technologies: Security Challenges and Possible Solutions," *Journal of Network and Computer Applications*, vol. 95, pp. 54–78, 2017.

[118] A. Gupta, R. K. Jha, and R. Devi, "Security Architecture of 5G Wireless Communication Network," *International Journal of Sensors Wireless Communications and Control*, vol. 8, no. 2, pp. 92–99, 2018.

[119] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security," *IEEE Security & Privacy*, vol. 14, no. 4, pp. 34–44, 2016.

[120] L. Wang, J. Liu, M. Chen, G. Gui, and H. Sari, "Optimization-Based Access Assignment Scheme for Physical-Layer Security in D2D Communications Underlaying a Cellular Network," *IEEE Transactions on Vehicular Technology*, 2018.

[121] M. Rahman and E. S. Al-Shaer, "Automated Synthesis of Distributed Network Access Controls: A Formal Framework with Refinement," *IEEE Transactions on Parallel & Distributed Systems*, no. 1, pp. 1–1, 2017.

[122] M. Khan, P. Ginzboorg, K. Järvinen, and V. Niemi, "Defeating the downgrade attack on identity privacy in 5g," in *International Conference on Research in Security Standardisation*. Springer, 2018, pp. 95–119.

[123] D. He, S. Chan, and M. Guizani, "Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 389–398, 2015.

[124] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, A. G. Reddy, K. Park, and Y. Park, "On The Design of Fine Grained Access Control with User Authentication Scheme for Telecare Medicine Information Systems," *IEEE Access*, vol. 5, pp. 7012–7030, 2017.

[125] S. Jha, N. Li, M. Tripunitara, Q. Wang, and W. Winsborough, "Towards Formal Verification of Role-Based Access Control Policies," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 4, pp. 242–255, 2008.

[126] Q. Huang, Y. Yang, and L. Wang, "Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things," *IEEE Access*, vol. 5, pp. 12 941–12 950, 2017.

[127] H. Qinlong, M. Zhaofeng, Y. Yixian, N. Xinxin, and F. Jingyi, "Improving Security and Efciency for Encrypted Data Sharing in Online Social Networks," *China Communications*, vol. 11, no. 3, pp. 104–117, 2014.

[128] N. Saxena, G. Tsudik, and J. H. Yi, "Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs," *IEEE Transactions on Parallel & Distributed Systems*, no. 2, pp. 158–170, 2008.

[129] A. Castiglione, A. De Santis, B. Masucci, F. Palmieri, A. Castiglione, J. Li, and X. Huang, "Hierarchical and Shared Access Control," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 850–865, 2016.

[130] S. Jarecki and N. Saxena, "On the Insecurity of Proactive RSA in the URSA Mobile Ad Hoc Network Access Control Protocol," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 739–749, 2010.

[131] D. Wang, Z. Wang, B. Shen, and F. E. Alsaadi, "Security-Guaranteed Filtering for Discrete-Time Stochastic Delayed Systems with Randomly Occurring Sensor Saturations and Deception Attacks," *International Journal of Robust and Nonlinear Control*, vol. 27, no. 7, pp. 1194–1208, 2017.

[132] J. You, Z. Zhong, G. Wang, and B. Ai, "Security and Reliability Performance Analysis for Cloud Radio Access Networks with Channel Estimation Errors," *IEEE Access*, vol. 2, pp. 1348–1358, 2014.

[133] M. Cheminod, L. Durante, L. Seno, and A. Valenzano, "Semiautomated Verification of Access Control Implementation in Industrial Networked Systems," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1388–1399, 2015.

[134] Y. Siriwardhana, P. Porambage, M. Liyanage, J. S. Walia, M. Matinmikko-Blue, and M. Ylianttila, "Micro-Operator driven Local 5G Network Architecture for Industrial Internet," in *IEEE Wireless Communications and Networking Conference (WCNC) 2019*. IEEE, 2019, pp. 1–8.

[135] A. Prasad, Z. Li, S. Holtmanns, and M. A. Uusitalo, "5G Micro-Operator NetworksA Key Enabler for New Verticals and Markets," in *Telecommunication Forum (TELFOR), 2017 25th*. IEEE, 2017, pp. 1–4.

[136] P. Ahokangas, S. Moqaddamerad, M. Matinmikko, A. Abouzeid, I. Atkova, J. F. Gomes, and M. Iivari, "Future Micro Operators Business Models in 5G," *The Business & Management Review*, vol. 7, no. 5, p. 143, 2016.

[137] P. P. Sriram, H.-C. Wang, H. G. Jami, and K. Srinivasan, "5G Security: Concepts and Challenges," in *5G Enabled Secure Wireless Networks*. Springer, 2019, pp. 1–43.

[138] J. Yao, Z. Han, M. Sohail, and L. Wang, "A Robust Security Architecture for SDN-Based 5G Networks," *Future Internet*, vol. 11, no. 4, p. 85, 2019.

[139] O. Mämmelä, J. Hiltunen, J. Suomalainen, K. Ahola, P. Mannersalo, and J. Vehkaperä, "Towards Micro-Segmentation in 5G Network Security," in *European Conference on Networks and Communications (EuCNC 2016) Workshop on Network Management, Quality of Service and Security for 5G Networks*, 2016.

[140] M. C. Dacier, H. Konig, R. Cwalinski, F. Kargl, and S. Dietrich, "Security Challenges and Opportunities of Software-Defined Networking," *IEEE Security & Privacy*, no. 2, pp. 96–100, 2017.

[141] Z. Yan, P. Zhang, and A. V. Vasilakos, "A Security and Trust Framework for Virtualized Networks and Software-Defined Networking," *Security and communication networks*, vol. 9, no. 16, pp. 3059–3069, 2016.

[142] J.-H. Lam, S.-G. Lee, H.-J. Lee, and Y. E. Oktian, "Securing Distributed SDN with IBC," in *Ubiquitous and Future Networks (ICUFN), 2015 Seventh International Conference on*. IEEE, 2015, pp. 921–925.

[143] L. Pasquale, C. Ghezzi, C. Menghi, C. Tsigkanos, and B. Nuseibeh, "Topology Aware Adaptive Security," in *Proceedings of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*. ACM, 2014, pp. 43–48.

[144] A. R. Prasad, S. Arumugam, B. Sheeba, and A. Zugenmaier, "3GPP 5g Security," *Journal of ICT Standardization*, vol. 6, no. 1, pp. 137–158, 2018.

[145] R. P. Jover and V. Marojevic, "Security and Protocol Exploit Analysis of the 5G Specifications," *IEEE Access*, vol. 7, pp. 24 956–24 963, 2019.

[146] R. Borden, J. Mooney, M. Taylor, and M. Sharkey, "Threat Information Sharing Under GDPR," *Scitech Lawyer*, vol. 15, no. 3, pp. 30–35, 2019.

[147] S. Ziegler, E. Evequoz, and A. M. P. Huamani, "The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities," in *Digital Business Models*. Springer, 2019, pp. 201–226.

[148] L. Sabatino and G. Sapi, "Online Privacy and Market structure: Theory and evidence," DICE Discussion Paper, Tech. Rep., 2019.

[149] R. v. Eijk, H. Asghari, P. Winter, and A. Narayanan, "The Impact of User Location on Cookie Notices (Inside and Outside of the European Union)," in *Workshop on Technology and Consumer Protection (ConPro'19)*, 2019.

[150] V. Saraswat, R. A. Sahu, G. Sharma, V. Kuchta, and O. Markowitch, "Public-Key Encryption with Integrated Keyword Search," *Journal of Hardware and Systems Security*, pp. 1–14, 2019.

[151] V. Torvinen, N. B. Henda, D. C. Zamora, P. K. Nakarmi, P. SAARINEN, and M. Wifvesson, "Subscription Concealed Identifier," Mar. 28 2019, uS Patent App. 16/200,037.

[152] C. Li and B. Palanisamy, "Privacy in Internet of Things: from Principles to Technologies," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 488–505, 2019.

[153] K. Yan, W. Shen, Q. Jin, and H. Lu, "Emerging Privacy Issues and Solutions in Cyber-Enabled Sharing Services: From Multiple Perspectives," *IEEE Access*, 2019.

[154] K. Norrman, M. Näslund, and E. Dubrova, "Protecting IMSI and User Privacy in 5G Networks," in *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*. ICST (Institute for Computer Sciences, Social-Informatics and , 2016, pp. 159–166.

[155] P. F. Scott, "Secrecy and surveillance: Lessons from the Law of IMSI Catchers," *International Review of Law, Computers & Technology*, pp. 1–23, 2019.

[156] A. Braeken, M. Liyanage, P. Kumar, and J. Murphy, "Novel 5G Authentication Protocol to Improve the Resistance against Active Attacks and Malicious Serving Networks," *IEEE Access*, 2019.

[157] M. Liyanage, I. Ahmad, M. Ylianttila, A. Gurtov, A. B. Abro, and E. M. de Oca, "Leveraging LTE Security with SDN and NFV," in *2015 IEEE 10th International Conference on Industrial and Information Systems (ICIIS)*. IEEE, 2015, pp. 220–225.

[158] M. A. Hasnat, S. T. A. Rurnee, M. A. Razzaque, and M. Mamun-Or-Rashid, "Security Study of 5G Heterogeneous Network: Current Solutions, Limitations and Future Direction," in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*. IEEE, 2019, pp. 1–4.

[159] I. Ahmad, M. Liyanage, S. Namal, M. Ylianttila, A. Gurtov, M. Eckert, T. Bauschert, Z. Faigl, L. Bokor, E. Saygun *et al.*, "New Concepts for Traffic, Resource and Mobility Management in Software-Defined Mobile Networks," in *2016 12th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*. IEEE, 2016, pp. 1–8.

[160] A. R. Abdou, P. C. van Oorschot, and T. Wan, "Comparative Analysis of Control Plane Security of SDN and Conventional Networks," *IEEE Communications Surveys & Tutorials*, 2018.

[161] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "Big Data Analysis-Based Secure Cluster Management for Optimized Control Plane in Software-Defined Networks," *IEEE Transactions on Network and Service Management*, vol. 15, no. 1, pp. 27–38, 2018.

[162] M. Liyanage, I. Ahmed, J. Okwuibe, M. Ylianttila, H. Kabir, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, and E. M. De Oca, "Enhancing Security of Software Defined Mobile Networks," *IEEE Access*, vol. 5, pp. 9422–9438, 2017.

[163] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, and A. Meddahi, "NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures," *IEEE Communications Surveys & Tutorials*, 2018.

[164] S. Lal, T. Taleb, and A. Dutta, "NFV: Security Threats and Best Practices," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211–217, 2017.

[165] T. Alharbi, A. Aljuhani, and H. Liu, "Holistic DDoS Mitigation Using NFV," in *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*. IEEE, 2017, pp. 1–4.

[166] I. Faynberg and S. Goeringer, "NFV Security: Emerging Technologies and Standards," in *Guide to Security in SDN and NFV*. Springer, 2017, pp. 33–73.

[167] B. Benjamin, J. Coffman, H. Esiely-Barrera, K. Farr, D. Fichter, D. Genin, L. Glendenning, P. Hamilton, S. Harshavardhana, R. Hom *et al.*, "Data Protection in OpenStack," in *Cloud Computing (CLOUD), 2017 IEEE 10th International Conference on*. IEEE, 2017, pp. 560–567.

[168] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network Function Virtualization: Challenges and Opportunities for Innovations," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90–97, 2015.

[169] R. Wojtczuk, "Poacher Turned Gamekeeper: Lessons Learned from Eight Years of Breaking Hypervisors," *Black Hat USA*, 2014.

[170] A. Aljuhani and T. Alharbi, "Virtualized Network Functions Security Attacks and Vulnerabilities," in *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*. IEEE, 2017, pp. 1–4.

[171] F. Reynaud, F.-X. Aguessy, O. Bettan, M. Bouet, and V. Conan, "Attacks Against Network Functions Virtualization and Software-Defined Networking: State-of-the-Art," in *NetSoft Conference and Workshops (NetSoft), 2016 IEEE*. IEEE, 2016, pp. 471–476.

[172] K. Leach, F. Zhang, and W. Weimer, "Scotch: Combining Software Guard Extensions and System Management Mode to Monitor Cloud Resource usage," in *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer, 2017, pp. 403–424.

[173] X. He and J. Tian, "A Trusted VM Live Migration Protocol in IaaS," in *Chinese Conference on Trusted Computing and Information Security*. Springer, 2017, pp. 41–52.

[174] S. Chen, X. Zhang, M. K. Reiter, and Y. Zhang, "Detecting Privileged Side-Channel Attacks in Shielded Execution With Déjá Vu," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. ACM, 2017, pp. 7–18.

[175] M. Jouini and L. B. A. Rabai, "Security Problems in Cloud Computing Environments: A Deep Analysis and a Secure Framework," in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2018, pp. 926–952.

[176] A. R. Riddle and S. M. Chung, "A Survey On the Security of Hpervisors in cloud computing," in *Distributed Computing Systems Workshops (ICDCSW), 2015 IEEE 35th International Conference on*. IEEE, 2015, pp. 100–104.

[177] M.-W. Shih, M. Kumar, T. Kim, and A. Gavrilovska, "S-NFV: Securing NFV States By Using SGX," in *Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*. ACM, 2016, pp. 45–48.

[178] S. R. Krishna and B. P. Rani, "Virtualization Security Issues and Mitigations in Cloud Computing," in *Proceedings of the First International Conference on Computational Intelligence and Informatics*. Springer, 2017, pp. 117–128.

[179] V.-G. Nguyen, A. Brunstrom, K.-J. Grinnemo, and J. Taheri, "SDN/NFV-Based Mobile Packet Core Network Architectures: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1567–1602, 2017.

[180] N. F. Virtualization, "NFV Security; Problem Statement," *ETSI NFV-SEC*, vol. 1, 2014.

[181] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A Survey of Security In Software Defined Networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 623–654, 2016.

[182] M. D. Firoozjaei, J. P. Jeong, H. Ko, and H. Kim, "Security Challenges With Network Functions Virtualization," *Future Generation Computer Systems*, vol. 67, pp. 315–324, 2017.

[183] M. Monshizadeh, V. Khatri, and A. Gurtov, "NFV Security Considerations For Cloud-Based Mobile Virtual Network Operators," in *Software, Telecommunications and Computer Networks (SoftCOM), 2016 24th International Conference on*. IEEE, 2016, pp. 1–5.

[184] M. Pattaranantakul, Y. Tseng, R. He, Z. Zhang, and A. Meddahi, "A First Step Towards Security Extension for NFV Orchestrator," in *Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*. ACM, 2017, pp. 25–30.

[185] B. Jaeger, "Security Orchestrator: Introducing a Security Orchestrator In the Context of The Etsi NFV Reference Architecture," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, vol. 1. IEEE, 2015, pp. 1255–1260.

[186] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang, "SecMANO: Towards Network Functions Virtualization (NFV) Based Security Management and Oorchestration," in *Trustcom/BigDataSE/I SPA, 2016 IEEE*. IEEE, 2016, pp. 598–605.

[187] L. R. Battula, "Network Security Function Virtualization (NSFV) Towards Cloud Computing With NFV Over Openflow Infrastructure: Challenges and Novel Approaches," in *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*. IEEE, 2014, pp. 1622–1628.

[188] C. Lorenz, D. Hock, J. Scherer, R. Durner, W. Kellerer, S. Gebert, N. Gray, T. Zinner, and P. Tran-Gia, "An SDN/NFV-Enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement." *IEEE communications magazine*, vol. 55, no. 3, pp. 217–223, 2017.

[189] C. Basile, A. Lioy, C. Pitscheider, F. Valenza, and M. Vallini, "A Novel Approach for Integrating Security Policy Enforcement With Dynamic Network virtualization," in *Network Softwarization (NetSoft), 2015 1st IEEE Conference on*. IEEE, 2015, pp. 1–5.

[190] E. Felstaine, O. Hermoni, and N. Sandlerman, "System, Method, and Computer Program for Managing Security In a Network Function Virtualization (NFV) Based Communication Network," Oct. 4 2016, uS Patent 9,460,286.

[191] T. Kumar, P. Porambage, I. Ahmad, M. Liyanage, E. Harjula, and M. Ylianttila, "Securing Gadget-Free Digital Services," *Computer*, vol. 51, no. 11, pp. 66–77, 2018.

[192] W. Abdul, Z. Ali, S. Ghouzali, B. Alfawaz, G. Muhammad, and M. S. Hossain, "Biometric Security Through Visual Encryption for Fog Edge Computing," *IEEE Access*, vol. 5, pp. 5531–5538, 2017.

[193] A. Rahman, E. Hassanain, and M. S. Hossain, "Towards A Secure Mobile Edge Computing Framework For Hajj," *IEEE Access*, vol. 5, pp. 11 768–11 781, 2017.

[194] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks," *IEEE Access*, vol. 5, pp. 25 408–25 420, 2017.

[195] S. Rathore, P. K. Sharma, A. K. Sangaiah, and J. J. Park, "A Hesitant Fuzzy Based Security Approach for Fog and Mobile-Edge Computing," *IEEE Access*, vol. 6, pp. 688–701, 2018.

[196] Y. He, F. R. Yu, N. Zhao, and H. Yin, "Secure Social Networks in 5G Systems with Mobile Edge Computing, Caching, and Device-To-Device Communications," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 103–109, 2018.

[197] D. He, S. Chan, and M. Guizani, "Security In The Internet of Things Supported By Mobile Edge Computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 56–61, 2018.

[198] J. Zhang, Z. Zhang, and H. Guo, "Towards Secure Data Distribution Systems In Mobile Cloud Computing," *IEEE Trans. Mob. Comput*, vol. 16, no. 11, pp. 3222–3235, 2017.

[199] A. Awad, A. Matthews, Y. Qiao, and B. Lee, “Chaotic Searchable Encryption for Mobile Cloud Storage,” *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 440–452, 2018.

[200] R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, “A Lightweight Secure Data Sharing Scheme For Mobile Cloud Computing,” *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 344–357, 2018.

[201] H. He, R. Li, X. Dong, and Z. Zhang, “Secure, Efficient and Fine-Grained Data access control mechanism for P2P storage cloud,” *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 471–484, 2014.

[202] J. Fu, Y. Liu, H.-C. Chao, B. Bhargava, and Z. Zhang, “Secure Data Storage and Searching for Industrial IoT By Integrating Fog Computing and Cloud Computing,” *IEEE Transactions on Industrial Informatics*, 2018.

[203] Z. Wen, J. Cała, P. Watson, and A. Romanovsky, “Cost Effective, Reliable and Secure Workflow Deployment Over Federated Clouds,” *IEEE Transactions on Services Computing*, vol. 10, no. 6, pp. 929–941, 2017.

[204] W. Zhang, Y. Lin, and G. Qi, “Catch You If You Misbehave: Ranked Keyword Search Results Verification In Cloud Computing,” *IEEE Transactions on Cloud Computing*, vol. 6, no. 1, pp. 74–86, 2018.

[205] J. Xiong, X. Liu, Z. Yao, J. Ma, Q. Li, K. Geng, and P. S. Chen, “A Secure Data Self-Destructing Scheme in Cloud Computing,” *IEEE Transactions on Cloud Computing*, no. 1, pp. 1–1, 2014.

[206] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, “A Secure Cloud Computing Based Framework For Big Data Information Management of Smart Grid,” *IEEE transactions on cloud computing*, vol. 3, no. 2, pp. 233–244, 2015.

[207] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega *et al.*, “Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks,” *IEEE Communications magazine*, vol. 55, no. 5, pp. 72–79, 2017.

[208] N. Alliance, “5G Security Recommendations Package 2: Network Slicing,” https://www.ngmn.org/fileadmin/user_upload/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf, 2016.

[209] E. Dotaro, “5G Network Slicing and Security,” *Transport*, vol. 2018, 2017.

[210] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, “Network Slicing in 5G: Survey and Challenges,” *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, 2017.

[211] J. M. Hamamreh, E. Basar, and H. Arslan, “OFDM-Subcarrier Index Selection for Enhancing Security and Reliability of 5G URLLC Services,” *IEEE Access*, vol. 5, pp. 25 863–25 875, 2017.

[212] H. Bai, L. Jin, and M. Yi, “Artificial Noise Aided Polar Codes for Physical Layer Security,” *China Communications*, vol. 14, no. 12, pp. 15–24, 2017.

[213] C. Zhang, J. Ge, Z. Xia, and H. Du, “Graph Theory Based Cooperative Transmission for Physical-Layer Security in 5G Large-Scale Wireless Relay Networks,” *IEEE Access*, vol. 5, pp. 21 640–21 649, 2017.

[214] G. Gomez, F. J. Martin-Vega, F. J. Lopez-Martinez, Y. Liu, and M. Elkashlan, “Uplink NOMA in Large-Scale Systems: Coverage and Physical Layer Security,” *arXiv preprint arXiv:1709.04693*, 2017.

[215] A. Arafa, W. Shin, M. Vaezi, and H. V. Poor, “Securing Downlink Non-Orthogonal Multiple Access Systems by Trusted Relays,” *arXiv preprint arXiv:1805.01449*, 2018.

[216] M. Forouzesh, P. Azmi, N. Mokari, and K. K. Wong, “Robust Physical Layer Security for Power Domain Non-orthogonal Multiple Access-Based HetNets and HUDNs, SIC Avoidance at Eavesdroppers,” *arXiv preprint arXiv:1806.02013*, 2018.

[217] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, “Physical Layer Security for 5G Non-Orthogonal Multiple Access in Large-Scale Networks,” in *Communications (ICC), 2016 IEEE International Conference on*. IEEE, 2016, pp. 1–6.

[218] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, “Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks.” *IEEE Trans. Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.

[219] B. He, A. Liu, N. Yang, and V. K. Lau, “On the Design of Secure Non-Orthogonal Multiple Access Systems,” *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2196–2206, 2017.

[220] S. Karachontzitis, S. Timotheou, I. Krikidis, and K. Berberidis, “Security-Aware Max–Min Resource Allocation in Multiuser OFDMA Downlink,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 529–542, 2015.

[221] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, “Physical Layer Security in Massive MIMO,” *arXiv preprint arXiv:1505.00396*, 2015.

[222] Y. Deng, L. Wang, K.-K. Wong, A. Nallanathan, M. Elkashlan, and S. Lambotharan, “Safeguarding Massive MIMO Aided Hetnets Using Physical Layer Security,” in *Wireless Communications & Signal Processing (WCSP), 2015 International Conference on*. IEEE, 2015, pp. 1–5.

[223] N. Mokari, S. Parsaeefard, H. Saeedi, P. Azmi, and E. Hossain, “Secure Robust Ergodic Uplink Resource Allocation in Relay-Assisted Cognitive Radio Networks,” *IEEE Transactions on Signal Processing*, vol. 63, no. 2, pp. 291–304, 2015.

[224] X. Zhu, B. Yang, C. Chen, L. Xue, X. Guan, and F. Wu, “Cross-Layer Scheduling for OFDMA-Based Cognitive Radio Systems with Delay and Security Constraints,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 12, pp. 5919–5934, 2015.

[225] M. Zhang and Y. Liu, “Energy Harvesting for Physical-Layer Security in OFDMA Networks,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 154–162, 2016.

[226] M. R. Abedi, N. Mokari, M. R. Javan, and H. Yanikomeroglu, “Limited Rate Feedback Scheme for Resource Allocation in Secure Relay-Assisted OFDMA Networks,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2604–2618, 2016.

[227] R. Saini, A. Jindal, and S. De, “Jammer-Assisted Resource Allocation in Secure OFDMA With Untrusted Users.” *IEEE Trans. Information Forensics and Security*, vol. 11, no. 5, pp. 1055–1070, 2016.

[228] M. Zhang, Y. Liu, and R. Zhang, “Artificial Noise Aided Secrecy Information and Power Transfer in OFDMA Systems,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 3085–3096, 2016.

[229] M. R. Abedi, N. Mokari, M. R. Javan, and H. Yanikomeroglu, “Secure Communication in OFDMA-Based Cognitive Radio Networks: An Incentivized Secondary Network Coexistence Approach,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1171–1185, 2017.

[230] “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 15),” https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296, 2017.

[231] E. Arikan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[232] R. G. Gallager, “Low density parity-check codes. mit press,” *MIT Press, Cambridge, MA*, 1963.

[233] U. S. S. S. Arachchillage, D. N. K. Jayakody, S. K. Biswash, and R. Dinis, “Recent Advances and Future Research Challenges in Non-Orthogonal Multiple Access for 5G Networks,” in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. IEEE, 2018, pp. 1–6.

[234] R. Khan, K. J. Dushantha Nalin, H. Pervaiz, and R. Tafazolli, “Modulation Based Non-Orthogonal Multiple Access for 5G Resilient Networks,” in *Globecom Workshops (GC Wkshps), 2019 IEEE*. IEEE, 2019, pp. 1–6.

[235] A. Rajaram, R. Khan, S. Tharranetharan, D. N. K. Jayakody, R. Dinis, and S. Panic, “Novel swipt schemes for 5g wireless networks,” *Sensors*, vol. 19, no. 5, p. 1169, 2019.

[236] Z. Xiang, Y. Cai, W. Yang, X. Sun, and Y. Hu, “Physical Layer Security of Non-Orthogonal Multiple Access in Cognitive Radio Networks,” in *Wireless Communications and Signal Processing (WCSP), 2017 9th International Conference on*. IEEE, 2017, pp. 1–6.

[237] N. Horiike, E. Okamoto, and T. Yamamoto, “A Downlink Non-Orthogonal Multiple Access Scheme Having Physical Layer Security,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 205, 2018.

[238] H. Zhang, N. Yang, K. Long, M. Pan, G. K. Karagiannidis, and A. Nallanathan, “Energy Efficient Resource Allocation for Secure NOMA Networks,” in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. IEEE, 2018, pp. 1–6.

[239] K. Hartmann and C. Steup, “The Vulnerability of UAVs to Cyber Attacks-An Approach to the Risk Assessment,” in *Cyber Conflict (CyCon), 2013 5th International Conference on*. IEEE, 2013, pp. 1–23.

[240] R. Mitchell and R. Chen, “Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles using behavior rule specifications,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 5, pp. 593–604, 2014.

[241] H. Sedjelmaci, S. M. Senouci, and N. Ansari, “A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-

Attacks in UAV Networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1594–1606, 2018.

[242] M. Sbeiti, N. Goddemeier, D. Behnke, and C. Wietfeld, "PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 1950–1964, 2016.

[243] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion Detection and Ejection Framework Against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 5, pp. 1143–1153, 2017.

[244] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-Aided Secure Communications With Cooperative Jamming," *IEEE Transactions on Vehicular Technology*, 2018.

[245] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng, "Robust Trajectory and Transmit Power Design for Secure UAV Communications," *arXiv preprint arXiv:1806.06396*, 2018.

[246] Q. Wang, Z. Chen, and H. Li, "Energy-Efficient Trajectory Planning for UAV-Aided Secure Communication," *China Communications*, vol. 15, no. 5, pp. 51–60, 2018.

[247] L. Xiao, C. Xie, M. Min, and W. Zhuang, "User-Centric View of Unmanned Aerial Vehicle Transmission Against Smart Attacks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3420–3430, 2018.

[248] L. Chen, S. Qian, M. Lim, and S. Wang, "An Enhanced Direct Anonymous Attestation Scheme with Mutual Authentication for Network-Connected UAV Communication Systems," *China Communications*, vol. 15, no. 5, pp. 61–76, 2018.

[249] K.-W. Huang and H.-M. Wang, "Combating the Control Signal Spoofing Attack in UAV Systems," *IEEE Transactions on Vehicular Technology*, 2018.

[250] A. Singandhupe, H. M. La, and D. Feil-Seifer, "Reliable Security Algorithm for Drones Using Individual Characteristics From an EEG Signal," *IEEE Access*, vol. 6, pp. 22 976–22 986, 2018.

[251] N. Zhao, F. Cheng, F. R. Yu, J. Tang, Y. Chen, G. Gui, and H. Sari, "Caching UAV Assisted Secure Transmission in Hyper-Dense Networks Based on Interference Alignment," *IEEE Transactions on Communications*, vol. 66, no. 5, pp. 2281–2294, 2018.

[252] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy Rate Analysis of UAV-Enabled mmWave Networks Using Matérn Hardcore Point Processes," *IEEE Journal on Selected Areas in Communications*, 2018.

[253] S. Gong, C. Xing, Z. Fei, and S. Ma, "Millimeter-Wave Secrecy Beamforming Designs for Two-Way Amplify-And-Forward MIMO Relaying Networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2059–2071, 2017.

[254] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, "Enhancing Secrecy with Multi-Antenna Transmission in Millimeter Wave Vehicular Communication Systems," *IEEE Trans. Veh. Technol*, vol. 66, no. 9, pp. 8139–8151, 2017.

[255] W.-Q. Wang and Z. Zheng, "Hybrid MIMO and Phased-Array Directional Modulation for Physical Layer Security in mmWave Wireless Communications," *IEEE Journal on Selected Areas in Communications*, 2018.

[256] Y. R. Ramadan and H. Minn, "Artificial Noise Aided Hybrid Precoding Design for Secure mmWave MISO Systems With Partial Channel Knowledge," *IEEE Signal Processing Letters*, vol. 24, no. 11, pp. 1729–1733, 2017.

[257] C. Wang and H.-M. Wang, "Physical Layer Security in Millimeter Wave Cellular Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5569–5585, 2016.

[258] Y. R. Ramadan, H. Minn, and A. S. Ibrahim, "Hybrid Analog–Digital Precoding Design for Secrecy mmWave MISO-OFDM Systems," *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 5009–5026, 2017.

[259] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure Communications in Millimeter Wave Ad Hoc Networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3205–3217, 2017.

[260] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On The Physical Layer Security Analysis of Hybrid Millimeter Wave Networks," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1139–1152, 2018.

[261] W. Zeng, J. Zhang, S. Chen, K. P. Peppas, and B. Ai, "Physical Layer Security over Fluctuating Two-Ray Fading Channels," *IEEE Transactions on Vehicular Technology*, 2018.

[262] W. Wu, X. Gao, Y. Wu, and C. Xiao, "Beam Domain Secure Transmission for Massive MIMO Communications," *IEEE Transactions on Vehicular Technology*, 2018.

[263] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Physical Layer Security in TDD Massive MIMO," *IEEE Transactions on Information Theory*, 2018.

[264] Y. Liu, H.-H. Chen, and L. Wang, "Secrecy Capacity Analysis of Artificial Noisy MIMO ChannelsAn Approach Based on Ordered Eigenvalues of Wishart Matrices," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 617–630, 2017.

[265] Q. Li and L. Yang, "Artificial Noise Aided Secure Precoding for MIMO Untrusted Two-Way Relay Systems With Perfect and Imperfect Channel State Information," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2628–2638, 2018.

[266] F. Zhu, F. Gao, H. Lin, S. Jin, J. Zhao, and G. Qian, "Robust Beamforming for Physical Layer Security in BDMA Massive MIMO," *IEEE Journal on Selected Areas in Communications*, 2018.

[267] X. Chen and Y. Zhang, "Mode Selection in MU-MIMO Downlink Networks: A Physical-Layer Security Perspective," *IEEE Systems Journal*, vol. 11, no. 2, pp. 1128–1136, 2017.

[268] N. Shlezinger, D. Zahavi, Y. Murin, and R. Dabora, "The Secrecy Capacity of Gaussian MIMO Channels with Finite Memory," *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1874–1897, 2017.

[269] Y. Cao, X.-Q. Jiang, H.-M. Wang, and E. Bai, "MIMO Wiretap Channels Based on Generalized Extended Orthogonal STBCs and Feedback," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2454–2463, 2018.

[270] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint Relay Selection and Power Allocation in Large-Scale MIMO Systems with Untrusted Relays and Passive Eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 341–355, 2018.

[271] Z. Kong, S. Yang, F. Wu, S. Peng, L. Zhong, and L. Hanzo, "Iterative Distributed Minimum Total MSE Approach for Secure Communications in MIMO Interference Channels," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 594–608, 2016.

[272] S. Timilsina, G. A. A. Baduge, and R. F. Schaefer, "Secure Communication in Spectrum-Sharing Massive MIMO Systems with Active Eavesdropping," *IEEE Transactions on Cognitive Communications and Networking*, 2018.

[273] S. Wang, W. Li, and J. Lei, "Physical-Layer Encryption in Massive MIMO Systems With Spatial Modulation," *China Communications*, vol. 15, no. 10, pp. 159–171, 2018.

[274] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, Florida: CRC Press, 1996.

[275] S. C. Dushantha Nalin K. Jayakody, John Thompson and S. Durrani, *Wireless Information and Power Transfer: A New Green Communications Paradigm*. Springer-Verlag New York, 2017.

[276] L. R. Varshney, "Transporting information and energy simultaneously," in *2008 IEEE International Symposium on Information Theory*, July 2008, pp. 1612–1616.

[277] H. Xing, K. Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: A paradigm of self-sustaining friendly jammers for secure af relaying," *IEEE Transactions on Signal Processing*, vol. 63, no. 24, pp. 6616–6631, Dec 2015.

[278] H. Xing, L. Liu, and R. Zhang, "Secrecy Wireless Information and Power Transfer in Fading Wiretap Channel," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 180–190, Jan 2016.

[279] F. Jameel, D. N. K. Jayakody, M. F. Flanagan, and C. Tellambura, "Secure Communication for Separated and Integrated Receiver Architectures in SWIPT," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2018, pp. 1–6.

[280] T. D. Ponnimbaduge Perera and D. N. K. Jayakody and S. K. Sharma and S. Chatzinotas and J. Li, "Simultaneous wireless information and power transfer (swipt): Recent advances and future challenges," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 264–302, Firstquarter 2018.

[281] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical Layer Security With RF Energy Harvesting in AF Multi-Antenna Relaying Networks," *IEEE Transactions on Communications*, vol. 64, no. 7, pp. 3025–3038, July 2016.

[282] J. Lin, Q. Li, J. Yang, H. Shao, and W.-Q. Wang, "Physical-Layer Security for Proximal Legitimate User and Eavesdropper: A Frequency Diverse Array Beamforming Approach," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 671–684, 2018.

[283] T. Xiong, W. Lou, J. Zhang, and H. Tan, "MIO: Enhancing Wireless Communications Security Through Physical Layer Multiple Inter-Symbol Obfuscation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1678–1691, 2015.

[284] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security Versus Reliability Analysis of Opportunistic Relaying," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 6, pp. 2653–2661, 2014.

[285] X. Fang, N. Zhang, S. Zhang, D. Chen, X. Sha, and X. Shen, "On Physical Layer Security: Weighted Fractional Fourier Transform Based User Cooperation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5498–5510, 2017.

[286] H. Zhang, T. Wang, L. Song, and Z. Han, "Interference Improves PHY Security for Cognitive Radio Networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 609–620, 2016.

[287] H. Moosavi and F. M. Bui, "Delay-Aware Optimization of Physical Layer Security in Multi-Hop Wireless Body Area Networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1928–1939, 2016.

[288] P.-W. Tsai, C.-W. Tsai, C.-W. Hsu, and C.-S. Yang, "Network Monitoring in Software-Defined Networking: A Review," *IEEE Systems Journal*, 2018.

[289] M. Liyanage, I. Ahmad, J. Okwuibe, E. M. de Oca, H. L. MAI, O. L. Perez, and M. U. Itzazelaia, "Software Defined Security Monitoring in 5G Networks," *A Comprehensive Guide to 5G Security*, pp. 231–243, 2018.

[290] M. Liyanage, J. Okwuibe, I. Ahmed, M. Ylianttila, O. L. Pérez, M. U. Itzazelaia, and E. M. de Oca, "Software Defined Monitoring (SDM) for 5G Mobile Backhaul Networks," in *Local and Metropolitan Area Networks (LANMAN), 2017 IEEE International Symposium on*. IEEE, 2017, pp. 1–6.

[291] T. Combe, W. Mallouli, T. Cholez, G. Doyen, B. Mathieu, and E. M. de Oca, "An SDN and NFV Use Case: NDN Implementation and Security Monitoring," in *Guide to Security in SDN and NFV*. Springer, 2017, pp. 299–321.

[292] H. L. Mai, T. Nguyen, G. Doyen, R. Cogranne, W. Mallouli, E. M. de Oca, and O. Festor, "Towards A Security Monitoring Plane for Named Data Networking and Its Application Against Content Poisoning Attack," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2018, pp. 1–9.

[293] H. L. Mai, M. Aouadj, G. Doyen, D. Kondo, X. Marchal, T. Cholez, E. M. de Oca, and W. Mallouli, "Implementation of Content Poisoning Attack Detection and Reaction in Virtualized NDN Networks," in *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 2018, pp. 1–3.

[294] G. Gardikis, I. Koutras, G. Mavroudis, S. Costicoglou, G. Xilouris, C. Sakkas, and A. Kourtis, "An Integrating Framework For Efficient NFV Monitoring," in *NetSoft Conference and Workshops (NetSoft), 2016 IEEE*. IEEE, 2016, pp. 1–5.

[295] H. Kim, S. Yoon, H. Jeon, W. Lee, and S. Kang, "Service Platform and Monitoring Architecture for Network Function Virtualization (NFV)," *Cluster Computing*, vol. 19, no. 4, pp. 1835–1841, 2016.

[296] D. Palmisano, P. L. Ventre, A. Caponi, G. Siracusano, S. Salsano, M. Bonola, and G. Bianchi, "D-STREAMONNFV-Capable Distributed Framework for Network Monitoring," in *Teletraffic Congress (ITC 29), 2017 29th International*, vol. 2. IEEE, 2017, pp. 30–35.

[297] C.-T. Yang, S.-T. Chen, J.-C. Liu, Y.-Y. Yang, K. Mitra, and R. Ranjan, "Implementation of a Real-Time Network Traffic Monitoring Service with Network Functions virtualization," *Future Generation Computer Systems*, vol. 93, pp. 687–701, 2019.

[298] S.-H. Shen, "An Efficient Network Monitor for SDN Networks," *ACM SIGMETRICS Performance Evaluation Review*, vol. 46, no. 2, pp. 95–96, 2019.

[299] E. Hugues-Salas, F. Ntavou, D. Gkounis, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Monitoring and Physical-Layer Attack Mitigation in SDN-Controlled Quantum Key Distribution Networks," *Journal of Optical Communications and Networking*, vol. 11, no. 2, pp. A209–A218, 2019.

[300] F. Guo, K. Yan, D. Black, K. M. Moriarty, L. Wan, and Q. Chen, "Network Monitoring Using Traffic Mirroring and Encapsulated Tunnel in Virtualized Information Processing System," Feb. 12 2019, uS Patent App. 14/292,183.

[301] A. H. Celdrán, M. G. Pérez, F. J. G. Clemente, and G. M. Pérez, "Automatic Monitoring Management for 5G Mobile Networks," *Procedia Computer Science*, vol. 110, pp. 328–335, 2017.

[302] T. Maksymyuk, S. Dumych, M. Brych, D. Satria, and M. Jo, "An IoT Based Monitoring Framework for Software Defined 5G Mobile Networks," in *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*. ACM, 2017, p. 105.

[303] C. Sauvanaud, K. Lazri, M. Kaâniche, and K. Kanoun, "Anomaly Detection and Root Cause Localization in Virtual Network Functions," in *Software Reliability Engineering (ISSRE), 2016 IEEE 27th International Symposium on*. IEEE, 2016, pp. 196–206.

[304] ——, "Towards Black-Box Anomaly Detection in Virtual Network Functions," in *Dependable Systems and Networks Workshop, 2016 46th Annual IEEE/IFIP International Conference on*. IEEE, 2016, pp. 254–257.

[305] J. Zhang, R. Gardner, and I. Vukotic, "Anomaly Detection in Wide Area Network Meshes Using two Machine Learning Algorithms," *Future Generation Computer Systems*, vol. 93, pp. 418–426, 2019.

[306] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Effective and Efficient Network Anomaly Detection System Using Machine Learning Algorithm," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 1, pp. 46–51, 2019.

[307] M. Wu, Z. Song, and Y. B. Moon, "Detecting Cyber-Physical Attacks in CyberManufacturing Systems with Machine Learning Methods," *Journal of intelligent manufacturing*, vol. 30, no. 3, pp. 1111–1123, 2019.

[308] A. Faigon, K. Narayanaswamy, J. TAMBULURI, R. Ithal, S. Malmskog, and A. Kulkarni, "Machine Learning based Anomaly Detection," Apr. 23 2019, uS Patent App. 10/270,788.

[309] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN Based Network Intrusion Detection System Using Machine Learning Approaches," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 493–501, 2019.

[310] S. Rezvy, Y. Luo, M. Petridis, A. Lasebae, and T. Zebin, "An Efficient Deep Learning Model for Intrusion Classification and Prediction in 5G and IoT Networks," in *2019 53rd Annual Conference on Information Sciences and Systems (CISS)*. IEEE, 2019, pp. 1–6.

[311] M. A. S. Monge, A. H. González, B. L. Fernández, D. M. Vidal, G. R. García, and J. M. Vidal, "Traffic-flow analysis for source-side DDoS recognition on 5G environments," *Journal of Network and Computer Applications*, 2019.

[312] P. Calyam and M. Swany, "Research Challenges in Future Multi-Domain Network Performance Measurement and Monitoring," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 3, pp. 29–34, 2015.

[313] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, and M. Ylianttila, "5G Privacy: Scenarios and Solutions," in *IEEE 5G World Forum (5GWF)*. IEEE, 2018.

[314] W. D. de Mattos and P. R. Gondim, "M-Health Solutions Using 5G Networks and M2M Communications," *IT Professional*, vol. 18, no. 3, pp. 24–29, 2016.

[315] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, "Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks," *IEEE Transactions on Smart Grid*, 2018.

[316] D. Liao, H. Li, G. Sun, M. Zhang, and V. Chang, "Location and Trajectory Privacy Preservation in 5G-Enabled Vehicle Social Network Services," *Journal of Network and Computer Applications*, vol. 110, pp. 108–118, 2018.

[317] R. Borgaonkar, A. Shaik, N. Asokan, V. Niemi, and J.-P. Seifert, "LTE and IMSI Catcher Myths," *BlackHat Europe*, vol. 2015, 2015.

[318] A. Taralika, D. Challa, S. Kumar, A. Ojha, and L. Chung, "Secure Authentication to Provide Mobile Access to Shared Network Resources," Apr. 12 2018, uS Patent App. 15/836,641.

[319] S. A. Aaronson, "Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows," *Centre for International Governance Innovation*, 2018.

[320] P. F. Edemekong and M. J. Haydel, "Health insurance portability and accountability act (hipaa)," in *StatPearls [Internet]*. StatPearls Publishing, 2018.

[321] P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, and I. Sanchez, "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services," *Computer Law & Security Review*, vol. 34, no. 2, pp. 193–203, 2018.

[322] I. Graef, "Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union," *Telecommunications Policy*, vol. 39, no. 6, pp. 502–514, 2015.

[323] "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield," {http://europa.eu/rapid/press-release_IP-16-216_en.htm}, 2016.

[324] B. Goodman and S. Flaxman, "European Union Regulations on Algorithmic Decision-Making and A "Right to Explanation"," *arXiv preprint arXiv:1606.08813*, 2016.

[325] A. Pfitzmann and M. Hansen, "A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, uUndetectability, Unobservability, Pseudonymity, and Identity Management," *PRIVACY AND DATA SECURITY*, 2010.

[326] P. Zhang, M. Durresi, and A. Durresi, “Mobile Privacy Protection Enhanced with Multi-access Edge Computing,” in *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2018, pp. 724–731.

[327] “Security in Telecommunications and Information Technology,” https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-SEC-2015-PDF-E.pdf, 2015.

[328] “SG17: Security,” https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx, 2019.

[329] “IP Wireless Access in Vehicular Environments (ipwave),” https://datatracker.ietf.org/wg/ipwave/documents/, 2018.

[330] P. Nikander and R. Moskowitz, “Host Identity Protocol (hip) Architecture,” 2006.

[331] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, “Authentication and Authorization for Constrained Environments (ACE),” *Internet Engineering Task Force, Internet-Draft draft-ietf-aceoauth-authz-07*, 2017.

[332] “Security for 5G,” https://tools.ietf.org/html/draft-naresh-mptcp-security-for-5g-00, 2018.

[333] “CYBER; Application of Attribute Based Encryption (ABE) for PII and Personal Data Protection on IoT Devices, WLAN, Cloud and Mobile Services - High Level Requirements ,” https://www.etsi.org/deliver/etsi_ts/103400_103499/103458/01.01.01_60/ts_103458v010101p.pdf, 2018.

[334] “CYBER; Attribute Based Encryption for Attribute Based Access Control,” https://www.etsi.org/deliver/etsi_ts/103500_103599/103532/01.01.01_60/ts_103532v010101p.pdf, 2018.

[335] “Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification,” https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/013/03.01.01_60/gs_NFV-SEC013v030101p.pdf, 2017.

[336] “P1912 - Standard for Privacy and Security Architecture for Consumer Wireless Devices,” https://standards.ieee.org/project/1912.html, 2015.

[337] “oneM2M; Security Solutions ,” {https://www.etsi.org/deliver/etsi_ts/118100_118199/118103/02.04.01_60/ts_118103v020401p.pdf}, 2016.

[338] “5G-ENSURE ,” https://5g-ppp.eu/5g-ensure/, 2017.

[339] “Mobile Platform Work Group (MPWG),” https://trustedcomputinggroup.org/work-groups/mobile/, 2015.

[340] S. Scott-Hayward, G. O’Callaghan, and S. Sezer, “SDN Security: A Survey,” in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN For*. IEEE, 2013, pp. 1–7.

[341] N. Alliance, “5G White Paper,” 2015.

[342] “Security Aspects of Network Capabilities Exposure in 5G ,” {https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2018/180921_NGMN-NCEsec_white_paper_v1.0.pdf}, 2018.

[343] “NIST Cloud Computing Security Reference Architecture ,” {https://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf}, 2013.

[344] NSF Projects. Available:https://www.nsf.gov/pubs/2018/nsf18572/nsf18572.htm. [Online; accessed June 03, 2019].

[345] 5G Ensure. Available:http://www.5gensure.eu/. [Online; accessed June 03, 2019].

[346] NSF projects. Available:https://www.nsf.gov/pubs/2018/nsf18570/nsf18570.htm. [Online; accessed June 03, 2019].

[347] NSF 5G projects. Available:https://www.nsf.gov/cise/5G/. [Online; accessed June 03, 2019].

[348] STEM Project. Available:https://nsf.gov/awardsearch/showAward?AWD_ID=1818942&HistoricalAwards=false. [Online; accessed June 03, 2019].

[349] 5G!Pagoda H2020 Project. Available:https://5g-pagoda.aalto.fi/. [Online; accessed June 03, 2019].

[350] 5G MiEdge H2020 Project. Available:https://5g-miedge.eu/. [Online; accessed June 03, 2019].

[351] 5G Champion Project. Available:http://www.5g-champion.eu/. [Online; accessed June 03, 2019].

[352] IRACON COST Project. Available:http://www.iracon.org/. [Online; accessed June 03, 2019].

[353] M. T. Hammi, E. Livolant, P. Bellot, A. Serhrouchni, and P. Minet, “A Lightweight IoT Security Protocol,” in *Cyber Security in Networking Conference (CSNet), 2017 1st*. IEEE, 2017, pp. 1–8.

[354] M. Villari, M. Fazio, S. Dustdar, O. Rana, and R. Ranjan, “Osmotic Computing: A New Paradigm for Edge/cloud Integration,” *IEEE Cloud Computing*, vol. 3, no. 6, pp. 76–83, 2016.

[355] T. Dimitrakos, “Security Challenges and Guidance for Protecting NFV on Cloud IaaS,” https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/05_NFVSECURITY/S01_CHALLENGES/HUAWEI_DIMITRAKOS.pdf, 2017.

[356] F. Kemmer, C. Reich, M. Knahl, and N. Clarke, “Software Defined Privacy,” in *Cloud Engineering Workshop (IC2EW), 2016 IEEE International Conference on*. IEEE, 2016, pp. 25–29.

[357] R. Khan, D. N. K. Jayakody, S. Vishal, K. Viney, K. Kuljeet, and C. Zheng, “A Machine Learning Based Energy-Efficient Non-Orthogonal Multiple Access Scheme,” in *International Forum on Strategic Technology*. IEEE, 2019, pp. 1–6.

[358] F. Pan, Z. Pang, M. Luvisotto, M. Xiao, and H. Wen, “Physical-Layer Security for Industrial Wireless Control Systems: Basics and Future Directions,” *IEEE Industrial Electronics Magazine*, vol. 12, no. 4, pp. 18–27, Dec 2018.

[359] F. Pan, H. Wen, R. Liao, Y. Jiang, A. Xu, K. Ouyang, and X. Zhu, “Physical Layer Authentication Based on Channel Information and Machine Learning,” in *2017 IEEE Conference on Communications and Network Security (CNS)*, Oct 2017, pp. 364–365.

[360] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, “PHY-Layer Spoofing Detection With Reinforcement Learning in Wireless Networks,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10 037–10 047, Dec 2016.

[361] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. A. Faruque, “Security trends and advances in manufacturing systems in the era of industry 4.0,” in *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Nov 2017, pp. 1039–1046.

[362] R. Taylor, D. Baron, and D. Schmidt, “The World in 2025-Predictions for the Next Ten Years,” in *Microsystems, Packaging, Assembly and Circuits Technology Conference (IMPACT), 2015 10th International*. IEEE, 2015, pp. 192–195.

[363] M. Samaniego and R. Deters, “Blockchain as a Service for IoT,” in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2016, pp. 433–436.

[364] O. Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT,” *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.

[365] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with iot. challenges and opportunities,” *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[366] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?” *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.

[367] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, “Provchain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability,” in *Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing*. IEEE Press, 2017, pp. 468–477.

[368] J. Park and J. Park, “Blockchain security in Cloud Computing: Use Cases, Challenges, and Solutions,” *Symmetry*, vol. 9, no. 8, p. 164, 2017.

[369] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “Blockchain-Based Database to Ensure data Integrity in Cloud Computing Environments,” in *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)*, 2017.

[370] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee, “Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks,” *IEEE Transactions on Parallel and Distributed Systems*, 2019.

[371] R. Brundo and R. De Nicola, “Blockchain-Based Decentralized Cloud/Fog Solutions: Challenges, Opportunities, and Standards,” *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 22–28, 2018.

[372] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, “Cloud/fog Computing Resource Management and Pricing for Blockchain Networks,” *IEEE Internet of Things Journal*, 2018.

[373] N. Pokrovskaia, “Tax, Financial and Social Regulatory Mechanisms Within the Knowledge-Driven Economy. Blockchain Algorithms and Fog Computing for the Efficient Regulation,” in *2017 XX IEEE International Conference on Soft Computing and Measurements (SCM)*. IEEE, 2017, pp. 709–712.

[374] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, “Secure and Energy-Efficient Handover in Fog Networks Using Blockchain-Based DMM,” *IEEE Communications Magazine*, vol. 56, no. 5, pp. 22–31, 2018.

[375] P. K. Sharma, M.-Y. Chen, and J. H. Park, “A software Defined fog Node Based Distributed Blockchain Cloud Architecture for IoT,” *IEEE Access*, vol. 6, pp. 115–124, 2018.

Rabia Khan works as a Research Engineer and a Ph.D candidate at National Research Tomsk Polytechnic University, Tomsk, Russia since October 2017. She has received MS degree in Telecom and Networks from Bahria University, Karachi, Pakistan, and received MSc. and BSc (Hons) degree in Physics from University of Karachi, Pakistan. Worked as a cooperative teacher at University of Karachi from 2009 to 2010. She has been awarded a full-time scholarship from Ministry of Russian Education, Russia for PhD. studies.

She serves as a reviewer in Elsevier, IEEE and other journals and conferences. Elsevier recognized her outstanding contribution in reviewing papers and awarded a certificate. Her research interests are NOMA, security, URLLC, smart cities and Machine learning in wireless communication systems.

Pardeep Kumar (M13) received the B.E. degree in computer science from Maharishi Dayanand University, Haryana (India), in 2002 and the M.Tech degree in computer science from Chaudhary Devilal University, Harnana (India), in 2006 and the Ph.D. degree in ubiquitous computing from Dongseo University, Busan (South Korea) in 2012. He is currently a Lecturer/Assistant Professor with the Department of Computer Science, Swansea University, Swansea, UK. From 2012 to 2018, he had held postdoc positions at the Department of Computer Science, Oxford University, Oxford UK (08/2016 - 09/2018), and at the Department of Computer Science, The Arctic University of Norway, Tromso, Norway (08/2015- 08/2016), and at Centre for Wireless Communications and the Department of Communications Engineering, University of Oulu, Finland (04/2012 to 08/2015). Dr. Kumar has published more than 40 research papers including including international journals (IEEE Communications Surveys and Tutorials, IEEE TIFS, IEEE Sensors, etc. IEEE CE) and conferences, and holds three patents. He is recipient of four times best paper awards from ubiquitous sensor network laboratory, Dongseo University, South Korea. Dr. Kumar's research interests include security in sensor networks, smart environments, cyber physical systems, body area networks, Internet of Things, and 5G networks.

Dushantha Nalin K. Jayakody (S09, M14 and SM'18) received the Ph. D. degree in Electronics, Electrical, and Communications Engineering, from the University College Dublin, Ireland in 2014. He received his MSc degree in Electronics and Communications Engineering from the Department of Electrical and Electronics Engineering, Eastern Mediterranean University, Turkey in 2010 (under the University full graduate scholarship) and ranked as the first merit position holder of the department, and B. E. electronics engineering degree (with first-class honors) in 2008 from Dawood University of Engineering & Technology, Pakistan and was ranked as the merit position holder of the University (under SAARC Scholarship.). From 2014 - 2016, he was a Postdoc Research Fellow at the Institute of computer science, University of Tartu, Estonia and Department of Informatics, University of Bergen, Norway. From 2016, he is a faculty member at the School of Computer Science & Robotics, National Research Tomsk Polytechnic University, Russia. Since summer 2017, he is a full professor at the National Research Tomsk Polytechnic University, Russia. Prof. Jayakody also serves as the Head of Research & Educational center on Automation and Information Technologies.

He spent a short research stays at Centre for Telecommunications Research, University of Sydney, Australia in 2015 and Texas A&M University at Qatar in 2018.

Prof. Jayakody has received the best paper award from the IEEE International Conference on Communication, Management and Information Technology (ICCMIT) in 2017 and International Conference on Emerging Technologies of Information and Communications, Bhutan, March 2019. In July 2019, Prof. Jayakody received the Sri Lanka Education Leadership Award. In 2017 and 2018, he received the outstanding faculty award by National Research Tomsk Polytechnic University, Russia.

Prof. Jayakody has published over 120 international peer reviewed journal and conference papers. His research interests include PHY and NET layer prospective of 5G communications technologies such as NOMA for 5G etc, Cooperative wireless communications, device to device communications, LDPC codes, Unmanned Ariel Vehicle etc. Prof. Jayakody is a Senior Member of IEEE and he has served as workshop chair, session chair or technical program committee member for various international conferences, such as IEEE PIMRC 2013-2019, IEEE WCNC 2014-2018, IEEE VTC 2015-2018 etc. He currently serves as a Area Editor the Elsevier Physical Communications Journal, MDPI Information journal and Wiley Internet of Technology Letters. In his career, so far, he has attracted nearly 4M $ research funding. Also, he serves as a reviewer for various IEEE Transactions and other journals.

Madhusanka Liyanage (S07, M16) is currently an Marie Curie Fellow at University Collage Dublin, Ireland. He is also an adjunct professor at the University of Oulu, Finalnd. He received his B.Sc. degree (First Class Honours) in electronics and telecommunication engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009, the M.Eng. degree from the Asian Institute of Technology, Bangkok, Thailand, in 2011, the M.Sc. degree from the University of Nice Sophia Antipolis, Nice, France, in 2011, and the Ph.D. degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. From 2011 to 2012, he worked a Research Scientist at the I3S Laboratory and Inria, Shopia Antipolis, France. He has been a Visiting Research Fellow at the Department of Computer Science, University of Oxford, Data61, CSIRO, Sydney, Australia, the Infolabs21, Lancaster University, U.K., and Computer Science and Engineering, The University of New South Wales during 2015-2018.

He has co-authored over 60 publications including three edited books with Wiley and one patent. He is the demo co-chair of WCNC2019 and publicity chair of ISWCS 2019. He served as a Technical program Committee Members at EAI M3Apps 2016, 5GU 2017, EUCNC 2017, EUCNC 2018, 5GWF 2018, MASS 2018, MCWN 2018, WCNC 2019, EUCNC 2019 conferences and Technical program co-chair in SecureEdge workshop at IEEE CIT2017 conference and Blockchain for IoT workshop at IEE Globecom 2018. He has also served as the session chair in a number of other conferences including IEEE WCNC 2013, CROWNCOM 2014, 5GU 2014, IEEE CIT 2017, IEEE PIMRC 2017, 5GWF 2018, Bobynet 2018, Globecom 2018. Moreover, He has received two best Paper Awards in the areas of SDMN security (at NGMAST 2015) and 5G Security (at IEEE CSCN 2017). Additionally, he has been awarded two research grants and 21 other prestigious awards/scholarships during his research career.

Dr. Liyanage has worked for more than twelve EU, international and national projects in ICT domain. He held responsibilities as a leader of work packages in several national and EU projects. Currently, he is the Finnish national coordinator for EU COST Action CA15127 on resilient communication services. In addition, he is/was serving as a management committee member for four other EU COST action projects namely EU COST Action IC1301, IC1303, CA15107, CA16226 and CA16116. Liyanage has over three years experience in research project management, research group leadership, research project proposal preparation, project progress documentation and graduate student co-supervision/mentoring, skills. In 2015, 2016, 2017 and 2018, he won the Best Researcher Award at the Centre for Wireless Communications, University of Oulu for his excellent contribution in project management and dissemination activities. Additionally, two of the research projects (MEVICO and SIGMONA projects) received the CELTIC and ITEA Excellence/innovation Awards in 2013, 2017, 2018 and 2019. Dr. Liyanage's research interests are 5G, SDN, IoT, Blockchain, MEC, mobile and virtual network security. Contact him at madhusanka@ucd.ie