IEEE

IEEE INGR

International Network Generations Roadmap

2022 Edition

Security and Privacy

IEEE Future NETWORKS

An IEEE 5G and Beyond Technology Roadmap

futurenetworks.ieee.org/roadmap

Table of Contents

Tables

Figures

ABSTRACT

The digital transformation brought on by 5G is redefining current models of end-to-end (E2E) connectivity and service reliability to include security-by-design principles necessary to enable 5G to achieve its promise. 5G trustworthiness highlights the importance of embedding security capabilities from the very beginning while the 5G architecture is being defined and standardized. Security requirements need to overlay and permeate through the different layers of 5G systems (physical, network, and application) as well as different parts of an E2E 5G architecture within a risk-management framework that takes into account the evolving security-threats landscape. 5G presents a typical use-case of wireless communication and computer networking convergence, where 5G fundamental building blocks include components such as Software Defined Networks (SDN), Network Functions Virtualization (NFV) and the edge cloud. This convergence extends many of the security challenges and opportunities applicable to SDN/NFV and cloud to 5G networks. Thus, 5G security needs to consider additional security requirements (compared to previous generations) such as SDN controller security, hypervisor security, orchestrator security, cloud security, edge security, etc. At the same time, 5G networks offer security improvement opportunities that should be considered. Here, 5G architectural flexibility, programmability and complexity can be harnessed to improve resilience and reliability.

The working group scope fundamentally addresses the following:

- 5G security considerations need to overlay and permeate through the different layers of the 5G systems (physical, network, and application) as well as different parts of an E2E 5G architecture including a risk management framework that takes into account the evolving security threats landscape.
- 5G exemplifies a use-case of heterogeneous access and computer networking convergence, which extends a unique set of security challenges and opportunities (e.g., related to SDN/NFV and edge cloud, etc.) to 5G networks. Similarly, 5G networks by design offer potential security benefits and opportunities through harnessing the architecture flexibility, programmability and complexity to improve its resilience and reliability.
- The IEEE FNI security WG's roadmap framework follows a taxonomic structure, differentiating the 5G functional pillars and corresponding cybersecurity risks. As part of cross collaboration, the security working group will also look into the security issues associated with other roadmap working groups within the IEEE Future Network Initiative.

Disclaimer: in this document we use 5G to refer to future networks including evolution such as B5G, 6G, etc.

Key words:

5G Cybersecurity, security, privacy, data protection, reliability, resilience, mMTC, URLLC, SDN/NFV, cyber risk assessment and management, threat scenarios, cyber-attacks, security controls, mitigation, defense.

CONTRIBUTORS

Ashutosh Dutta	John's Hopkins University / Applied Physics Lab, Security Working Group Co-Chair
Eman Hammad	Texas A&M University – RELLIS, Security Working Group Co-Chair
Michael Enright	Quantum Dimension, Inc.
Fawzi Behmann	IEEE ComSoc North America Regional Board, TelNet Management Consulting, Inc.
Arsenia Chorti	ENSEA, CNRS
Ahmad Cheema	Shared Services Canada
Kassi Kadio	Shared Services Canada
Julia Urbina-Pineda	IEEE HKN Member and CyberIIoT CEO
Khaled Alam	Rogers Communications (Formerly)
Ahmed Limam	Higher Institute of Engineering and Technology (ESPRIT)
Fred Chu	University of California, Los Angeles
John Lester	Our Lady of Fatima University Valenzuela, Philippines
Jong-Geun Park	Seoul National University of Science and Technology
Joseph Bio-Ukeme	Carleton University
Sanjay S Pawar	Usha Mittal University of Technology
Roslyn Layton	Aalborg University
Prakash Ramchandran	Intel
Kingsley Okonkwo	Chevron
Lyndon Ong	Ciena
Marc Emmelmann	Fraunhofer FOKUS
Omneya Issa	Department of National Defence, Canada
Rajakumar Arul	Amrita Vishwa Vidyapeetham
Sireen Malik	T-Mobile
Sivarama Krishnan	National Library of Medicine
Suresh Sugumar	Intel Corporation
Tk Lala	ZecureZ Consulting Company
Matthew Borst	IEEE Future Networks Initiative
Brad Kloza	IEEE Future Networks Initiative

INGR ROADMAP

1. INTRODUCTION

5G technologies provide ubiquitous connectivity while also addressing the demands of both individual consumers and businesses [1]. 5G technologies are expected to provide higher throughput, lower latency, a higher density and mobility range without compromising reliability. By virtue of its flexibility and an agile development methodology that uses modular network functions, it supports various use cases that are both scalable and cost effective. 5G can support exciting new use cases, including IoT, smart transportation, e-Health, smart cities, tactile computing and kinesthetic communication, and holographic interactions. 5G introduces a paradigm shift into wireless mobile communication [1].

Not only is 5G evolutionary (providing higher bandwidth and lower latency than current-generation technology), more importantly, 5G is revolutionary in that it is expected to enable fundamentally new applications with much more stringent requirements in latency (e.g., real time) and bandwidth (e.g., streaming). 5G could help solve the last-mile/-kilometer problem and provide broadband access to the next billion users on earth at a much lower cost because of its use of new spectrum and its improvements in spectral efficiency [1] [2] [3]. An alternative view of the use-cases and innovation that will be driven by 5G is illustrated by Figure 1. The Figure differentiates between four advanced capabilities of 5G that are directly relating to innovation:

- Massive Content: cellular network data rates increase about 10x every five years and that's going to leap ahead with 5G. This has big implications for mobile data networks.
- Massive IoT: 5G will enable connectivity of sensors, devices, objects, and so forth in a massive Internet of Things network.
- Massive Control: 5G will enable us to build infrastructure for remote controls, often known as, "tactile Internet." This means we can have an interaction with virtual environments just as we are used to from tactile interaction with objects around us, which means real and virtual object will be able to interact with a reaction time of one to 10 milliseconds to enable a human to control things in a steady state that mimics reality.
- Massive Resilience: in order to provide the massive sensing, massive IoT and massive control (low latency type applications) the network needs to be flexible and adaptive enough. SDN, NFV, Cloud RAN, Mobile Edge Cloud, Network Slicing are some of the functions that are needed to support flexibility and availability.

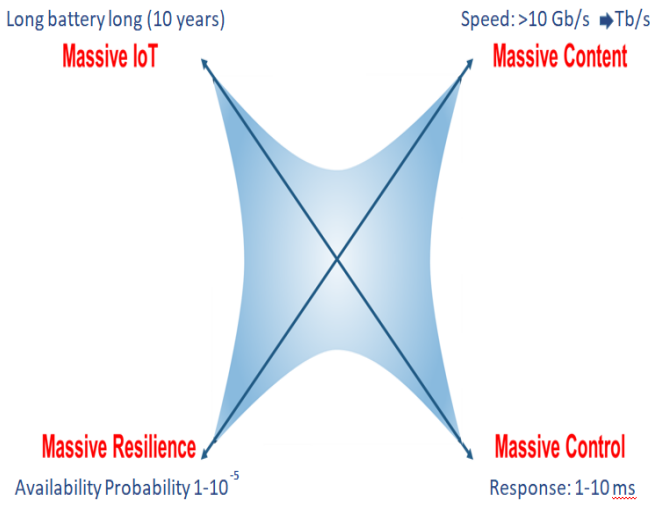

Figure 1. Key dimensions of 5G Networks, courtesy of 5G Lab Germany [4].

In order to support various 5G use-cases and applications, there is a critical need to design a secure and trusted end-to-end network [5]. 5G networks need to be flexible, adaptive, scalable and able to dynamically react to the changes in the network quite rapidly. To better understand the security risks and implications, this document proposes an approach to dividing the complex 5G ecosystem into domains/pillars to facilitate a more focused discussion of the security threats and risks. This would help better model and assess the cyber risks to the 5G network itself and to 5G-enabled use-cases. The progress of the 5G and beyond revolution may well be hindered if security issues are not tackled early on while the systems are being designed, standardized and deployed [2].

SDN and NFV are among the main technologies needed in order for 5G to support 5G-type applications. SDN/NFV typically includes additional network components including: SDN controller, Orchestrator, Hypervisor, Security Function Virtualization, all of which can introduce security risks. In addition to SDN/NFV specific components, there are other network functions such as cloud RAN, Mobile Edge Cloud (MEC) and Network Slicing that enable optimal resource sharing and support low latency applications. However, these additional network functions also give rise to additional security risks.

Various standards bodies including 3GPP, IEEE, and ETSI have been looking into security issues for 5G networks. Cao et al. [6] provide a survey of security aspects of 5G networks as defined in 3GPP. These authors present an overview of the network architecture and security functionality of the 3GPP's 5G networks and focus on the new features and techniques including the support of massive Internet of Things (IoT) devices, Device to Device (D2D) communication, Vehicle to Everything (V2X) communication, and network slice.

ETSI NFV security working group [7] group has developed different security specifications including problem statement, best current practice for security virtualization, security monitoring and management specification, security for VNFs. However, those specifications have not involved any end-to-end threat analysis of 5G network, nor do these specifications discuss the security opportunities of 5G. 5GPP Ensure project [8] has developed 5G-ENSURE architecture for 5G networks that revises the 3GPP security architecture from TS 33.401 and integrates key features and the domain concept to support trust models for a 5G beyond vision.

The INGR Security Roadmap 2021 Edition extends the First Edition released in 2020 complimenting previous content and providing a systems approach to security by analyzing the threats at various parts of the network and discussing the security pillars in more detail. The chairs of the INGR Security WG published part of the roadmap content in the IEEE 5G World Forum 2020 [9]. The roadmap working group considers the high-level view in Figure 2 in its treatment of the topic. It is paramount to consider this view to distinguish both challenges and opportunities.

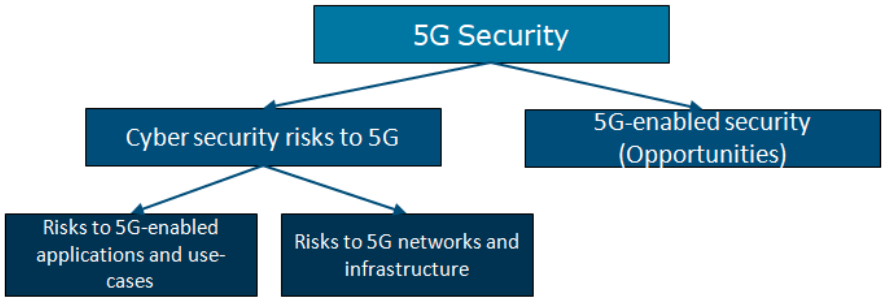

Figure 2. 5G & Beyond: Security Perspective, the progress of the 5G and beyond revolution may well be hindered if security issues are not tackled early on while the systems are being designed, standardized and deployed.

1.1. 2022 Edition Update

A summary of the main changes and updates in this document is listed below:

- 3.4 Summary of Working Group 2021 Activities
- 4 IEEE Security Standardization Efforts
- 6.4 Future Threat Landscape
- 7.5 Satellite
- 7.10 Physical Layer security
- 8.6 Quantum-Ready Security
- 9 Standardization Opportunities

2. WORKING GROUP VISON

2.1. The Big Picture for Security

Security and privacy must be the integral part that matures and evolves alongside technology and its applications. As these technologies are integrated into our daily life, such as smart homes, smart cities and critical infrastructures (e.g., smart grids, transportation, etc.), there will be a need to develop and integrate security controls at every layer of the communication system governing them. Security will cater to the need from large-scale constrained environments such as Industrial IoT use cases to individual premises network such as smart home.

In 3 years, 5G will have been standardized, and 30% deployment will have been completed. In 5 years, 5G will be fully deployed and will be looking at limitations or any services that have not been implemented in 5G. In 10 years, fully working 5G and beyond will be available, where any product/device can be used for communication and there will be no need for mobile phones and SIM

cards (e.g., smart devices with a camera), and there will be more video-based calls than traditional voice. There will be a massive increase in machine-to-machine type communication, and increased location-based services. Then the challenge would be how to provide fast, reliable and cheap wireless communication and connectivity everywhere. A single antenna array will be used for multiple communications protocols. And service providers would be able to provide seamless handovers between different networks (5G to wireless local area network (WLAN)) based on quality of service (QoS), pricing, or user preference during an ongoing communication (voice, video, data transmission). 5G and beyond will be able to withstand sophisticated cyber-attacks and continue to be available and functioning with minimal impact by providing resilient and flexible services.

2.2. Vision for a Successful Future Network Industry

Security will have extended up the stack to the application level (all end-point-to-end-point communications, whether those endpoints are people, systems, or simply two applications on a single machine). Security will have extended down the stack to the physical layer (PHY) level and below, for physical layer security.

Physical and virtual identity of people and things, and controlled access among them, will be key. In essence, all security can be formulated as an identity and access control problem.

Augmented reality, fully autonomous vehicles, smart infrastructures (e.g., home, cities, grids, healthcare, emergency services, etc.) and possible citizen united network or community-based networks, deployed and operated by volunteers are some of the compelling use cases. A low-latency, high-data rate and highly reliable network will be the norm rather than the exception. End-devices will be plug and play in a heterogeneous ecosystem.

2.3. 3-, 5-, and 10-Year's Goals

3 years: Most security will continue to be network-based and encryption will play a key role. Risk-based adaptive identity management and access control usage will grow, though not pervasively. Computational intelligence processing/artificial intelligence/machine learning (CI/AI/ML) will be applied increasingly—though reactively, if rapidly—to accelerate and improve all the traditional security functions (intrusion detection, fraud detection and management, etc.). Some security systems incorporate trust platforms such as block chain for identity.

5 years: 50/50 mix of application-level and network-level security will be available. Risk-based adaptive identity management and access control are applied in about a third of the market. CI/AI/ML is increasingly applied proactively thereby changing the security processes and security systems themselves. 20+% of systems incorporate trust platforms such as block chain for identity.

10 years: 90+% of security will involve full stack (PHY to APP layers). Risk-based adaptive identity management and access control are applied in 98% of the market. 98+% of security involves fully embedded CI/AI/ML, and those semi-autonomous and autonomous security systems will operate in both cooperative and fully contested modes. 90+% of systems incorporate trust platforms such as block chain for identity that is fully decentralized.

2.4. Security's Projected Impact

Beyond 5G, the biggest opportunity and challenge will be to finish an overall industry transformation to a software-centric vision (software defined network (SDN), network function virtualization (NFV), Fog, slicing) in which commercial off-the-shelf (COTS) network equipment is flexible and can be easily designed, implemented, deployed, upgraded, managed, maintained, and programmed using AI/ML as part of agility of all lifecycle management of network systems. The next-generation network will be heterogeneous in nature with a modular architecture, interoperable protocols and reconfigurable communication systems.

Consequently, next-generation networks security needs to be automated with a modular architecture (security as a service) that is negotiable, resilient and flexible depending upon the application, service provider and customer requirements and underlying network characteristics. We will have object-oriented cognitive security, such as humans identify humans, and similarly smart objects can identify other objects based on forge-resistance features or critical parameters.

Security will have extended up the stack to the application level (all end-point-to-end-point communications, whether those endpoints are people, systems, or simply two applications on a single machine). Security will also have extended down the stack to the PHY level and below, for physical layer security.

Controlled access and interaction among the physical and virtual identity of the people and things will be a key factor. This will be largely defined as identity and access control problem.

The fundamental questions that security would need to address is how could 5G systems function across all its layers (PHY to Application and Systems) as designed and planned in a trusted manner. Trusted identity of users, devices and applications have the right access to the right resources at the right time and data is managed efficiently and securely. Further, 5G will need to include cyber resilience as a fundamental objective in the systems design from hardware to application.

2.5. Scope of Working Group Effort

This security roadmap framework follows a certain taxonomy, differentiating the 5G functional pillars and corresponding cybersecurity risks. Figure 1 below depicts some of the 5G security pillars considered in this framework.

The First Edition of the security roadmap implicitly considered a hierarchal architecture model. This 2021 Edition discusses the security architecture in more detail specifically following an OSI-type model with multi-layer security paradigm. This 2021 Edition also aligns with a cybersecurity framework such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) to better outline a security reference architecture in terms of the security capabilities (Identify, Protect, Detect).

In the short term, 5G can support existing and evolving use cases such as the IoT, smart transportation, eHealth, smart cities, entertainment services, etc. Each of these verticals will address various security concerns. For example, we provide some of those use cases and security concerns associated with these use cases

- IoT—As 5G will enable more than 1,000 times more mobile data vs. today's cellular system by 2020, it is expected that it will serve as the cornerstone enabling the industrial IoT. In other words, 5G will help support IoT's communications needs on both IoT sensor and control networks.

    - Security concerns—As 5G supports the estimated scale of varying classes of IoT (e.g., industrial IoT, consumer IoT, infrastructure IoT), the following threat and cyber risks need to be considered: Distributed denial of service (DDoS) attacks from a large number of IoT manipulated devices that may render the system unavailable for critical services. Such attacks could be initiated as part of a larger cyber malicious activity.

- Smart transportation—Short latency and short-wave communication are essential operational requirements for emerging autonomous driving. Vehicles could be alerted to dangerous situations in real time and avoid collisions with intelligent emergency braking or steering systems. 5G plays an integral role in helping connect the vehicle-to-vehicle (V2V), vehicle-to-everything (V2X) architectures, coupled with other communication structures, to enable efficient and safe autonomous experience.
    - Security concerns—Success of smart transportation and autonomous vehicles requires strong security controls to ensure prevention/mitigation of any exploitation that may impact the safety of humans and infrastructure systems that are part of the ecosystems. 5G security controls should ensure that operational requirements are satisfied and that any threats emanating from the vehicles via the V2X connectivity are properly and efficiently managed.
- eHealth—With 5G's nearly real-time response times, doctors could perform operations around the world with video controls and machines to respond with limited delay. The medium, enabling coupling of robotics and sensors (among other technologies), will benefit from low latency and the ability to handle scale with higher bandwidths in a secure connection. Further, 5G may offer the possibility to realize "zero physical distance" from patient to accessible and more affordable healthcare without quality reduction. Wireless sensor networks would provide the ability to remotely monitor parameters, such as heart rate and blood pressure through the use of sensors.
    - Security Concerns—In order to support low-latency applications, security contexts need to be stored in the edge cloud to reduce delays due to authentication. However, this will increase the security vulnerability and hence, additional measures are needed. Additional security concerns include sensitive data privacy to ensure patient's data is protected.
- Smart cities—5G stands to undergird smart cities in which intelligent stoplights monitor and control traffic and proactive capabilities' emergency management systems are enabled. Multi-level parking facilities could communicate with in-car navigation systems to guide drivers to the best parking spaces and prevent traffic jams; service workers could quickly assess power outages while simply wearing smart contact lenses or glasses, etc.
    - Security Concerns—Device-to-device communications will be based on API-based security and will follow a service-oriented approach. Hence, countermeasures for API-based security vulnerabilities will need to be explored.
- Entertainment services—Current 4G cannot economically support such bandwidth-hungry applications, however, 5G could support interactive mobile games. For example, sporting events could utilize effective and efficient usage of spectrum and leverage new broadcast capabilities, such as 4D.
    - Security Concerns—Man-in-the-middle attacks, spoofing, impersonation, theft-of-service are some of the security concerns that need to be dealt with.

- Tactile computing and kinesthetic communication—The introduction of this technology, coupled with 5G, could make it possible to hold mobile devices next to accident victims to provide doctors with a tactile sense to aid diagnosis. For example, emergency rooms could be quickly prepared for immediate surgery, and life-saving opportunities could be enhanced by ensuring the right specialists are on hand.
    - Security Concerns—Device-to-device security will play a prominent role in this situation. Security parameters need to be modified properly to provide the desired level of service level agreement.
- Holographic interactions—For a variety of use cases, the ability to interact with a hologram and receive tactile responses presents an incredible future. For example, the ability to interact socially changes considerably as the zero-latency concept shifts from simply a Tweet as an interaction to actually being able to shake hands and see the person saying the comments directly. This also provides opportunities to reduce the global spread of diseases such as MERS, Ebola and other contagions.
    - Security Concerns—Identity management and authentication play an important role here. It is also important to provide data integrity, both the data at rest and data in motion.

This 2021 Edition of the framework focuses on the following.

- Alignment with NIST Cyber Security Framework
- 5G security architecture and requirements
- Risk-based adaptive/proactive security SDN/NFV orchestration and optimization
- Optimization guidelines on the foundational trade-offs: security vs. performance, and privacy vs. functionality

Discussion of example use-cases in more depth

- Expanded outline of 5G security topics including but not limited: physical Security, hardware security, etc.
- Security standardization opportunities
- Introduction to data sharing platforms and privacy

2.6. Linkages and Stakeholders

The Security Roadmap is a horizontal roadmap that integrates with most referenced stakeholders as a key and essential enabler. Of note here, security will provide input and guidance for stakeholders including carriers/providers, vendors, end-user applications and services, government agencies (Defense Advanced Research Projects Agency (DARPA), Department of Defense (DoD), etc.), R&D (academia, industry)

The Security Roadmap working group (WG) will need to share and coordinate with the following other INGR roadmap teams to ensure roadmap alignment:

- Standardization Building Blocks—Identify key 5G-specific areas that need security standardization, utilize rapid reaction standardization activity (RRSA) and Standards Forum to

mature and formalize security ideas, survey existing security standards, and security requirements.

- Millimeter Wave (mmWave) and Signal Processing—Assess security risks in mmWave compared to other types of radio access network (RAN) technology (e.g., long-term evolution (LTE), Wi-Fi) or access mechanism such as non-orthogonal multiple access (NOMA).
- Hardware—Identify hardware security requirements that can supplement/complement software security.
- Massive MIMO—Assess the security risks related to threat vectors such as eavesdropping, jamming, hijacking, and consider security-by-design approaches, such as physical security and system level.
- Applications and Services—Consider multi-layer security for different kinds of applications and use cases (e.g., IoT, remote surgery). Consider application-specific security requirements.
- Edge Automation Platform—Considerations of how edge automation could enable security for low-latency use-cases. For example, faster authentication will be required to support ultra-low latency applications, which would introduce additional vulnerabilities. Hence, additional security monitoring support would be needed.
- Satellite—Is terrestrial security enough? What are additional security issues for satellite such as jamming, spoofing etc.?
- Testbed—Need a dedicated security testbed to try out different types of security use cases by emulating the attack environment.

INGR roadmap teams mentioned above should coordinate with the Security roadmap team to recognize the opportunities where Security can be integrated with proper controls and performance considerations.

Table 1. Standards Organizations

Forum	Forum
IETF	Network Virtualization Overlay, Dynamic Service Chaining, Network Service Header
IEEE	IEEE 802 LAN/MAN, IEEE Future Network Initiative
3GPP	Mobility and Security Architecture and Specification, SA3 This working group defines the architecture
ITU	Defines the architecture for IMT 2020 and Key Performance Indicator (KPI)
NGMN	Defines the use cases for various pillars
ETSI ISG NFV	NFV Platform/Deployment Standards – Security, Architecture/Interfaces, Reliability, Evolution, Performance
ONF	OpenFlow SDN Controller Standards

Forum	Forum
OPNFV	NFV Open Platform/eCOMP/OPNFV Community TestLabs
Openstack	Cloud Orchestrator Open Source
OpenDaylight	Brownfield SDN Controller Open Source
ONOS	OpenFlow SDN Controller Open Source
DPDK/ODP	CPU/NIC HW API – Data Plane Development Kit
KVM Forum	Hypervisor
OVS	Open Source vSwitch
Linux	Operating System, Container Security, ONAP
ATIS/NIST/FCC/CSA	Regulatory Aspects of SDN/NFV

Enabling Technologies and Organizational Capabilities (Education, Regulators, Infrastructures, Policy)

- Industry and academia—Further development is needed to achieve computationally feasible and tamper-proof trust platforms, AI/ML algorithms for predictive/protective security decision making, cross-domain anomaly detection, data sharing platforms with privacy controls, etc.
- Standards and regulatory—An end-to-end security requires a strongly coordinated and agile standards development including the different standardization bodies. An additional standardization effort might be required to provide governance, align and synchronize 5G security standardization efforts to ensure minimal gaps, if any.
- Open Source/API community—It is important to make sure that the Open-Source software goes through proper review process and there is proper documentation available. The code also needs to be reviewed thoroughly. There is a need for static and dynamic software analysis tools to identify the vulnerability.
- Government—Security and Privacy compliance should be strictly enforced (lessons can be taken from Energy and Utilities industry).

2.7. Working Group Summary of Activities

During 2021, the security working group initiated and participated in several activities to promote and enhance awareness of the working group objective and efforts:

- 1st INGR Security Workshop: was held during March 2021 virtually for 3 half days. The workshop hosted invited and open call presentations, in addition to several panels.

- 5G World Forum Topical: The working group members proposed, organized and facilitated a topical under the title: "5G Security: Opportunities and Challenges". In this topical, we had 10 invited talks.
- 5G World Forum Working Groups Panel: the security working group participated in a joint panel with the Edge Services and AI/ML working groups.
- Launch of Physical Layer Security Focus Group: the focus group kicked its effort strongly and is continuing to work to structure the path forward for potential next steps. A main goal of this focus group is to identify clear and feasible PLS standardization efforts.
- CFP for a Tech Focus Security Special Collection: the working group continues to encourage relevant contributions in the form of white and technical papers. Within that effort we initiated a CFP for a Tech Focus Security Special Collection and opened the CFP for the interested community.
- The chairs and members of the working groups also participated in several other activities such as giving invited talks, presenting in panels in other workshops and conferences

3. TODAY'S LANDSCAPE

3.1. Current State of Technology and Research

The current security technology landscape is not fully adapted to 5G and beyond, further it is a fast and dynamically changing landscape. Security controls continue to evolve as 5G matures and evolves, which motivates a continuous assessment of security technologies that would best match the requirements within a risk-management framework.

Difficult Challenges

- **Identity and access management**—Are essential to achieve an end-to-end security of 5G and beyond. In general, authentication and encryption affect the performance for the delay sensitive applications. Hence, in order to support ultra-low latency types of applications without compromising the security, there is a need to provide faster authentication. This can be achieved by storing security context at the edges of the network or by authenticating the end users at the edges of the network. However, this gives rise to additional security vulnerability as the edges are typically distributed and may not be part of the core network. Further development on this is required.
- **Edge computing**—Is instrumental to enable 5G agnostic connectivity and low-latency use-cases. Fast authentication, trust management, controls on storage and transfer of sensitive security contexts on the edge are a few of the issues that need to be addressed. In addition, standards development for edge devices must evolve to enable tamper proofing, API security, etc.
- **Standards and policy**—Development regarding encryption and security certificate (key) management in 5G needs to evolve to ensure a seamless user experience for the different use-cases and across carriers/slices.
- **Resilience**—Cross-layer development incorporating security constraints in the design must be adopted in a top-down approach to improve 5G resilience on the system level.

- **Data security and privacy**—A high scale of data will be stored and used to enable and support 5G system operation and the application use-cases. This data must be classified and managed appropriately within a proper data management framework and security controls for at-rest and in-transit. Privacy should be taken into account in the 5G function design to determine if private information (such as Personally Identifiable Information – PII) needs to be collected, stored or shared. There needs to be a defined framework for secure and governed data sharing. The utilization of data trust models can also facilitate the sharing of non-PII data.
- **Network Slicing Security**—Scenarios that would introduce some required cross functionality between slices, such as if a user equipment (UE) that can consume services from multiple slices needs to be further examined from a cyber-risk perspective, and proper controls be put in place to ensure the mitigation of any risks when this function is enabled.

Standardization Opportunities

This roadmap identifies the following areas that would benefit from standardization:

- Formalization of application security requirements to support KPIs and SLAs
- AI/ML security
- Security interoperability considerations between operators including encryption and certificate management to support seamless QoE.
- Guidelines on security controls orchestration / optimization.

Security Roadmap Engagement with Other Organizations

This roadmap identifies the need to engage the following set of expertise in future developments:

- Standards liaisons—From the different standards entities including 3GPP.
- Cybersecurity subject matter experts (SMEs)—For continuous assessment of security architecture/standards, to advice on current landscape of technology, trends and future projections of capabilities and challenges.
- Regulatory champions
- Industry and academic representatives—To provide comprehensive insights on future evolution of threats, risk and solutions. Additionally, to provide guidance on potential solutions fitness, effectiveness and feasibility
- Future Networks Initiatives workgroups—To ensure that security is aligned with the functional requirements from other workgroups, and to ensure that potential impacts/adjustment of functionality include security as input.

4. FUTURE STATE (2032)

4.1. Reference Architecture

3GPP (Reference TS 33.501) has defined Security architecture that can be used as a reference architecture for various types of applications. Figure 3 shows the reference security architecture as defined in 3GPP.

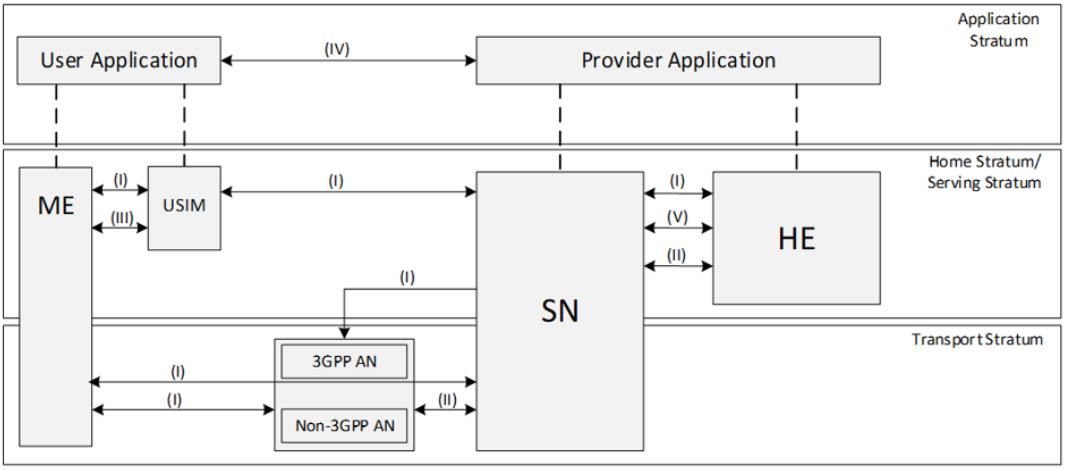

Figure 3. 3GPP security architecture

- Network access security (I): the set of security features that provide users with secure access to services, and which in particular protect against attacks on the (radio) access link.
- Network domain security (II): the set of security features that enable nodes to securely exchange signaling data, user data (between AN and SN and within AN), and protect against attacks on the wireline network.
- User domain security (III): the set of security features that provide secure access to mobile stations.
- Application domain security (IV): the set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- Visibility and configurability of security (V): the set of features that enable the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.
- SBA domain security (V): the set of security features that enable network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains. Such features include network function registration, discovery, and authorization security aspects, as well as the protection for the service-based interfaces. SBA domain security is a new security feature compared to TS 33.401 [10].
- Visibility and configurability of security (VI): the set of features that enable the user to be informed whether a security feature is in operation or not.

The IEEE Security working group will use this as a security reference architecture and will overlay various security threats as these apply to various domains and various verticals. The IEEE Security working group looks at various 5G enablers and highlights the opportunities and challenges associated with these enablers. The paper also elaborates the risk factors and a few potential mitigation techniques associated with these threats.

5. FOUNDATIONAL CONCEPTS

5.1. System Setup and Threat Model

This section describes an end-to-end 5G system model that includes various components in user plane, control plane, data plane, interfaces, and protocols. It is important to understand various threat vectors and devise potential mitigation techniques for each of these threats. Based on the existing security controls and risk factors, appropriate mitigation techniques can be developed accordingly.

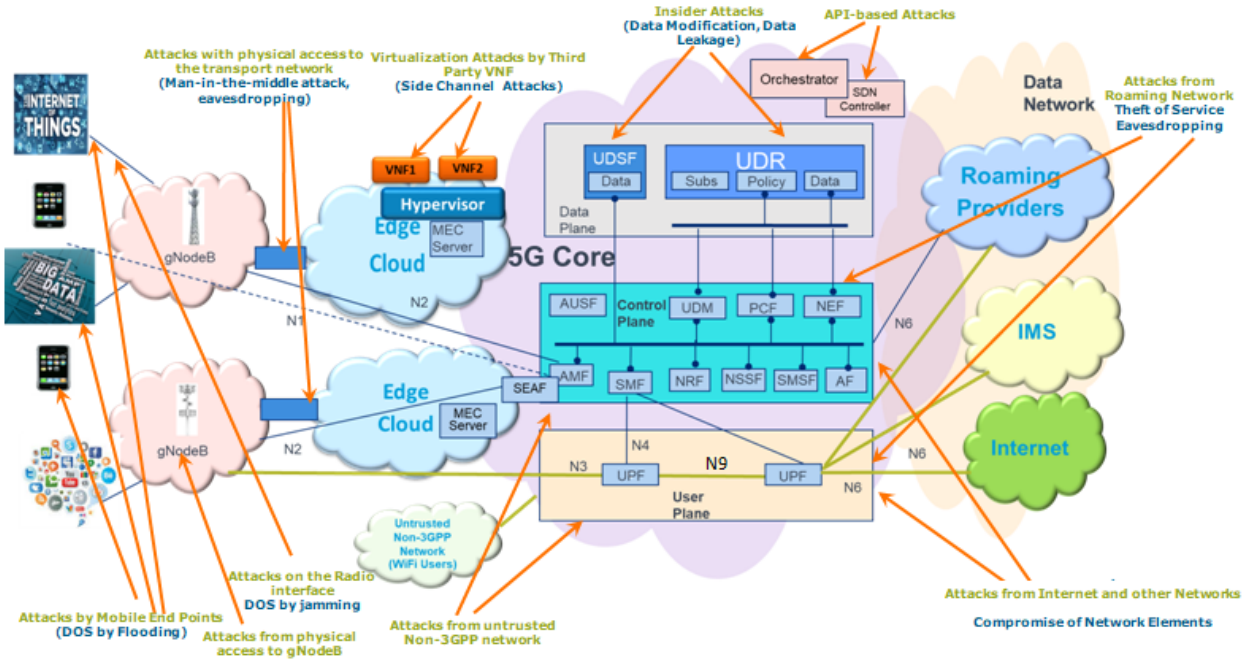

Figure 4. 5G Threat Model

Figure 4 helps illustrate a few examples of 5G threat vectors, including points of attack of various points of the 5G network. The figure also highlights the potential sources of attacks (threat actors) in the network [10] [11]. These attacks could come from many sources such as end devices, un-trusted networks (e.g., Wi-Fi), roaming networks, Internet, application service providers. Knowledge about the types of attacks and network assets that could be targeted helps to define the mitigation techniques.

Table 1 lists different types of cyber-attacks and a description of how attackers can launch such attacks. T1 through T10 illustrates different types of threat categories. These are categorized as loss of availability, loss of confidentiality, loss of integrity, loss of control, loss of integrity, loss of control, malicious insider, and theft of service, respectively. The attackers can launch these types of attacks by various means and pose threats to the network assets. Later in this roadmap document we expand on a few examples of threats and associated risk scenarios, for example, parts of the 5G Network. For example, an attacker can launch a denial-of-service attack and make the network unavailable by flooding a specific network interface, or crashing a network element. An attacker may also change the configuration of the network element through a management interface. There are also theft of service type attacks and malicious insider attacks that need to be dealt with.

While Table 1 describes different types of attacks and how an attacker could potentially execute these attacks, mitigation techniques are not addressed here. Various types of mitigation techniques and security controls can be developed to take care of each of these threats. Operators and service providers can analyze these potential threats and devise their mitigation techniques accordingly. Hence, a careful analysis of potential threats is needed, and mitigation techniques need to be developed based on associated risk factors. Tables II, III and IV in the following sections, highlight associated cyber risks and propose relevant mitigation techniques. Specifically, those tables consider threats associated with cloud RAN, mobile edge cloud and network slicing.

Table 2. Selected 5G threat Scenarios

No.	Category	Threat	Description
T1	Loss of Availability	Flooding an interface	Attackers flood an interface resulting in DoS condition (e.g., multiple authentication failure on s6a, DNS lookup)
T2		Crashing a network element	Attackers crash a network element by sending malformed packets
T3	Loss of Confidentiality	Eavesdropping	Attackers eavesdrop on sensitive data on control and bearer plane
T4		Data leakage	Unauthorized access to sensitive data on the server (HSS profile, etc.)
T5	Loss of Integrity	Traffic modification	Attackers modify information during transit (DNS redirection, etc.)
T6		Data modification	Attackers modify data on network element (change the NE configurations)
T7	Loss of Control	Control the network	Attackers control the network via protocol or implementation flaw
T8		Compromise of network element	Attackers compromise a network element via management interface
T9	Malicious Insider	Insider attacks	Insiders make data modification on network elements, make unauthorized changes to NE configuration, etc.
T10	Theft of Service	Service free of charge	Attackers exploit a flaw to use services without being charged

5.2. Cybersecurity Frameworks

5G networks security and privacy issues are best studied through a structured and methodological approach especially when considering the complexity, interdependence and sensitivity of the different ecosystems. A cybersecurity framework is a series of guidelines defining the best practices to manage the cybersecurity risk. Such frameworks aim to reduce an organization or system exposure to vulnerabilities [12].

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [12] is one of the most widely adopted frameworks. The framework categorizes cybersecurity capabilities under five main functions as shown in Figure 5 below.

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

793 × 475

Figure 5. NIST CSF Framework [12].

This framework will guide the development of the roadmap recommendations and future editions.

5.3. Cyber Risk Management Framework and Methodology

Cyber threats to 5G networks will continue to change and evolve resulting in increased challenges for security engineering and defense. Cyber risk management (CRM) enables system owners, operator and security teams to better understand what threats could impact their systems and the scale and type of impact successful threats could instigate on those systems. Moreover, CRM helps structure the defense mechanisms to disrupt the kill-chain of the considered risk scenarios. For example, considering a risk scenario related to DoS attacks caused by malicious IoT on the cloud RAN, a proper threat modeling and risk assessment would shed light on the best mitigation approaches that would either eliminate the threat or reduce its impact.

The cyber risk of a certain threat against part of the system or the end-to-end system can be accessed through the knowledge of few key factors in a process called risk assessment which is illustrated in Figure 6. The main factors that would help assess the level of risk include 1) the probability of the threat scenario, and 2) the business impact caused by the threat under consideration: Risk = Probability x Impact. The risk scenario probability can be assessed as a function of the systems vulnerabilities, exposure, current threats, and any existing mitigating controls that may adjust the probability that the threat could be successful, as illustrated in Figure 7 [13].

For specific areas of the 5G systems which are of high impact, a select number of threat scenarios are considered for which a high-level risk assessment is presented as in later sections.

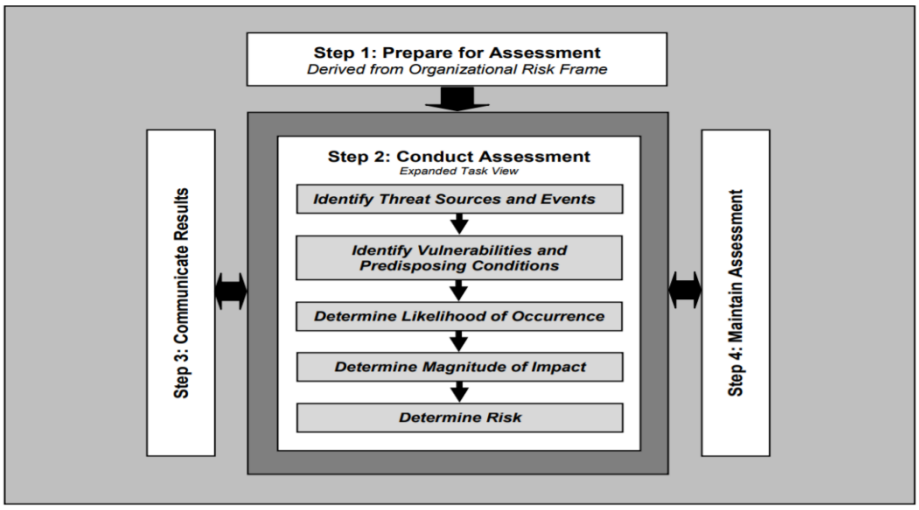

Figure 6. Risk assessment process [13].

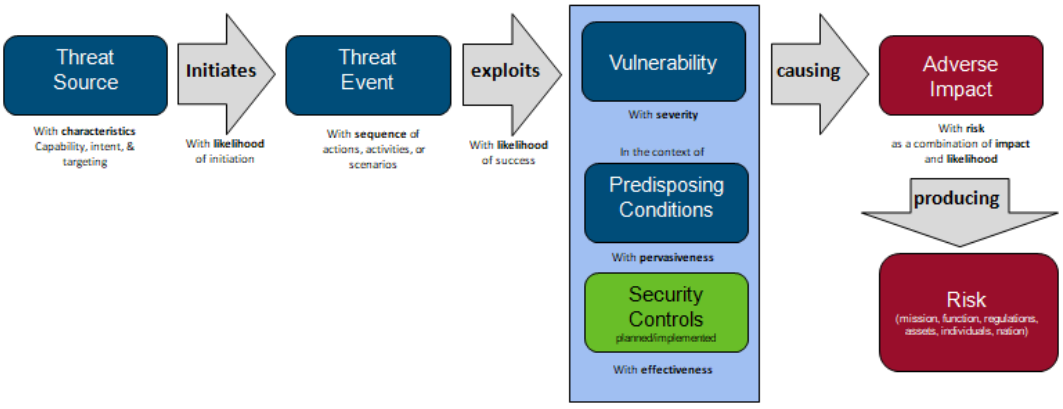

Figure 7. Generic risk model with key factors [13].

6. Security and Privacy Domains

This work proposes establishing a high-level framework to enable a holistic approach for studying 5G end-to-end security for vertical use-cases. At the base of this approach is distinguishing between different security domains/pillars for 5G networks which will help focus on both 1) identifying system vulnerabilities as well as associated risks, and 2) envisioning suitable mitigation techniques. Figure 8 illustrates the security pillars identified by this work thus far, where 5G security needs to take into account all those pillars and their interdependencies. We elaborate on some of those below:

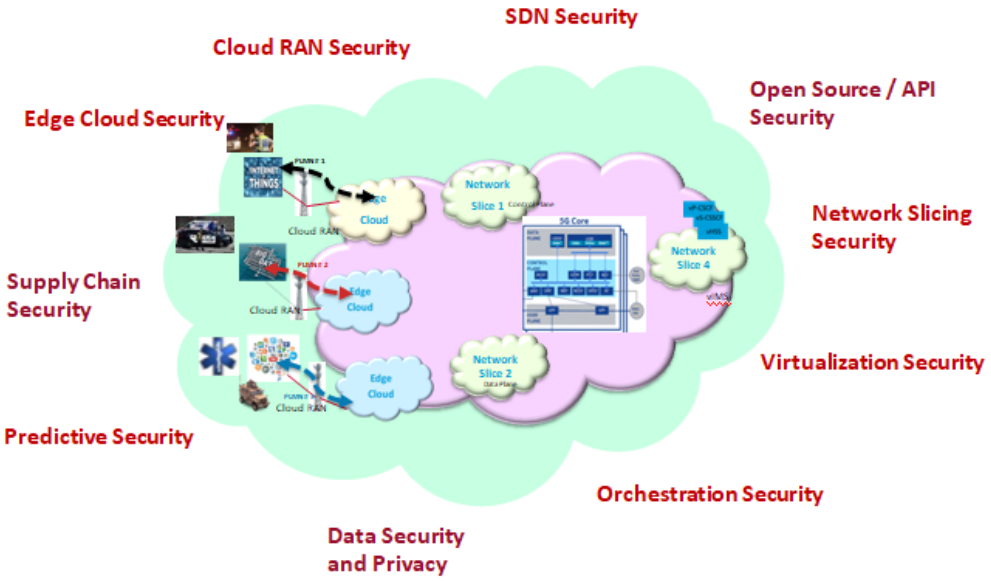

Figure 8. 5G Security Pillars

6.1. Management and Orchestration Security

5G resource allocation and optimization complexity levels have motivated the increased utilization of AI/ML algorithms in the management and orchestration layer (network, service, slice, etc.). For example, in an SDN/NFV environment, the orchestrator provisions virtual network functions (VNFs) based on the network condition and network intelligence. For example, in case of overload or security attacks, the orchestrator is notified of the condition of the network and communicates with the SDN controller that in turn controls the firewalls and routers to stop the attacks. At the same time, the orchestrator can help to scale out by instantiating additional VNFs. As the attack subsides, the orchestrator can scale down the VNFs. While the orchestrator adds the flexibility, there is also potential vulnerability for the orchestration. An attacker can use legitimate access to the orchestrator and manipulate its configuration in order to run a modified VNF, or alter the behavior of the VNF through changing its configuration through the orchestrator. Alternatively, the attacker can hijack the VNF placement procedure and place a VNF in a rogue place. Some of the mitigation techniques include deployment of some of the inherent best current practices for orchestration security by way of detection mechanism when the separation is violated; provide secure logging for access; automate system or configuration auditing. Deployment of a security monitoring system can detect the compromised VNF separation, any kind of anomaly in the system or provide an alert mechanism when some critical configuration data in the orchestrator is altered. Access control, file system protection, system integrity protection and hardening of separation policy through proper configuration management are some other mitigation mechanisms.

6.1.1. Virtualization / Softwarization Security

With the advent of virtualization, application of hypervisors and containers are becoming more prevalent. While these technologies allow multiple tenants and virtual network functions to reside on the same physical hardware, these also expose various security issues such as data exfiltration, resource starvation, side channel attacks, VM-based attacks through east-west and north-south traffic. For

example, a hypervisor may be compromised somehow by the attacker. The attacker can then use hypervisor privilege to install kernel root kit in VNF's operating system (OS) and thereby can control and modify the VNF. Some of the mitigation techniques that can be applied include hypervisor introspection scheme and hypervisor hardening mechanisms that can protect hypervisor's code and data from unauthorized modification and can guard against bugs and misconfigurations in the hardened hypervisors. The use of software vulnerability management procedures can also make sure the hypervisor is secured from attacks. Security function virtualization allows many of the security functions, namely DDOS, intrusion detection system (IDS), intrusion prevention system (IPS), and firewall functionalities to be virtualized. This allows an operator to deploy a dynamic security framework without depending upon proprietary hardware and software from various vendors. An operator or enterprise owner can potentially instantiate the virtualized security functions from various vendors and dynamically service chain them on demand. This will help to reduce the capital expenditure and operational expenditure. However, successful service chaining depends upon the orchestrator, SDN controller, network controller, and security orchestrator. Thus, all those security vulnerabilities are also applicable while providing a successful security function virtualization. Since security function virtualization also includes certain automation techniques, false-positive aspects need to be considered as well. Figure 9 shows potential security issues with virtualization.

Potential Security Challenges	Potential Mitigation	Risk Severity	Threat Likelihood
Lack of visibility into Network Traffic	API-based monitoring Embed security monitoring in the Hypervisor		
Execution of VMs with different Trust levels	Firewalls should be used to isolate VM groups from other groups for east-west traffic		
VNF Catalog is compromised	Apply encryption for Data at Rest Harden Access Control		
Communication between VNF Catalog, Orchestrator, and Virtual Infrastructure Manager is compromised	API Security Hardening Security monitoring		
Wrong placement of VNF	Verification of VNF placement API Security		

Figure 9. Potential security issues with virtualization

Threat 1: Attack from VMs in the same domain

- VM would be manipulated by attackers and potentially extend the attack to other VMs
- Buffer overflow, DOS, ARP, Hypervisor, vswitch

Threat 2: Attack to host, hypervisor and VMs from applications in host machine

- Poor design of hypervisors, improper configuration
- Attackers inject malicious software to virtual memory and control VM
- Malformed packet attacks to hypervisors

Threat 3: Attack from host applications communicating with VMs

- Host applications being attacked can initiate monitoring, tampering or DOS attack to communications going through host vSwitch
- Improper network isolation, Improper configuration to application privileges of host machine
- Lack of restriction to services or application

Threat 4: Attack to VMs from remote management path

- Outside attackers could initiate communication by eavesdropping, tampering, DOS attack, and Man-in-the-Middle attack
- Gain illegal access of the system and access OS without authorization, tamper and obtain sensitive and important information of a system
- Poor design and development of the application may lead to many known attacks (e.g., buffer overflow attacks)

Threat 5: Attack to external communication with 3rd party applications

- The API interface accessed by 3rd party applications in the untrusted domains is easily subject to malicious attack. Such attack includes illegal access to API, DOS attack to API platform
- Logical bugs in APIs, API authentication/authorization mechanism problems and security policy configuration problems.

Threat 6: Attack from external network via network edge node

- Virtualized Firewalls, Residential gateways

Threat 7: Attack from host machines or VMs of external network domain

- VNF migration, VNF scaling (Scale in- Scale out)

Use Case: Hypervisor gets compromised somehow by the attacker. Attacker uses hypervisor privilege to install kernel root kit in VNF's OS and thereby controls and modifies the VNF.

Mitigation Techniques:

- Hypervisor Introspection schemes can use the Hypervisor's higher privilege to secure the guest VMs.
- A Hypervisor-based introspection scheme can detect guest OS rootkit that got installed by the attacker.
    - Adoption of Hypervisor hardening mechanisms can protect hypervisor's code and data from unauthorized modification and can guard against bugs and misconfigurations in the hardened hypervisors.

- Use Software vulnerability management procedure to make sure the hypervisor is secured from attack

Here is a list of potential security opportunities from Virtualization.

- Provides resiliency in the event of DDOS attack by way of closed loop automation
- Multi-tenant operation
- Sharing of resources to support priority applications
- Ability to scale up and scale down the network based on the load in the network
- Distributed inventory control

6.1.2. SDN Security

SDN controller enables dynamic security control based on the intelligence gathered through north-bound API and then controlling the routers and switches through south bound API. This adds resilience to the network and mitigates the attacks quickly. However, the SDN controller can be subjected to attacks through its north bound and south bound interface. There is also potential risk of bugs and misconfiguration and source code vulnerability that needs to be taken into account. There are potential north-bound and south-bound API-based attacks for the SDN controller. Some of the attacks include denial of service attacks through south bound interface; REST API parameter exploitation through north-bound API; north-bound API flood attack; man-in-the middle attack (MiTM) spoofing; protocol fuzzing through south-bound API, and SDN controller impersonation through south-bound API. Proper mitigation mechanisms need to be put in place to detect these kinds of attacks and take appropriate mitigation techniques to keep the SDN controller operational.

Potential Security Challenges	Potential Mitigation	Risk Severity	Threat Likelihood
Denial of service attack through South Bound Interface	• Security monitoring • Access control		
REST API Parameter Exploitation (North Bound API)	• API Authentication • SDN controller Code Scanning • System Logging and Auditing		
North Bound API Flood Attack	• API Monitoring • Closed Loop Automation		
Man-In-The Middle Attack (Spoofing Attack)	• SDN Scanner • Closed Loop Automation		
Protocol Fuzzing Attack (South Bound API)	• Hardening mechanism for SDN Controller		
Controller Impersonation (South Bound API)	• Access Control • API monitoring		

High
Medium
Low

Figure 10. SDN Security - Select Cyber Risk Scenarios and Potential Mitigations

SDN Security Opportunities:

- SDN controller provides resilience to the attack and overload

SDN controller can interact with North Bound API and South Bound API to learn the network condition and can scale-up or scale-down the network resources accordingly. This will help to make the network more resilient.

- Enhances programmability and adaptability for the network routers and firewalls

Using South Bound interface, the SDN controller can configure the routers and firewalls using open flow protocols

- Facilitates dynamic service chaining for closed loop automation

By way of dynamic service chaining approach, SDN controller can work in conjunction with the orchestrator and data analytics module and can service chain various security function virtualizations, namely DDOS, IDS, and IPS and provide automation to detect and mitigate the attacks.

- Provides Dynamic Security Control mechanism to stop attacks on signaling plane and data plane

IDS can find out the details of the attackers such as IP address, IMEI, IMSI, location etc. in the signaling and data plane. These data are passed onto the SDN controller. SDN controller in turn has the ability to put the firewall rules and stop these attacks in the signaling and control plane.

6.1.3. Network Slicing Security

While network slicing enables sharing the resources in the network more efficiently and helps to allocate resources to support different types of applications, these also give rise to security concerns. However, from a security perspective, proper security controls must be implemented to ensure proper isolation of slices and enabling virtualization infrastructure. This includes slice categorization and adequate provisioning of resources. For example, critical network slices should not be co-located with slices dedicated for less-trusted or untrusted services. Further, strong security controls must be implemented to limit and secure information flow between slices. This would prevent and mitigate many threats such as side channel attacks across slices, DoS attack via virtual resources depletion, etc.

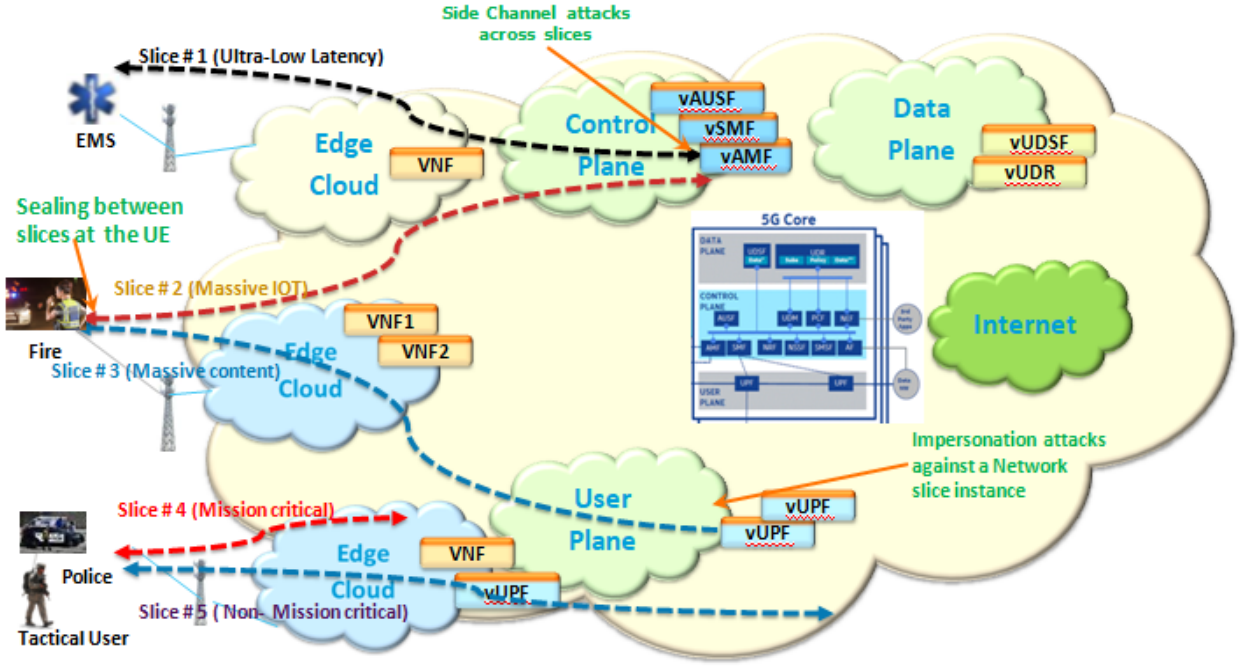

Figure 11. Network Slicing Security

Potential Security Challenges	Potential Mitigation	Risk Severity	Threat Likelihood
Different security protocols or policies in different slices results in higher probability of attack	• Adequate isolation of slices with different security levels • Separate authentication of a UE accessing multiple slices at once	Medium	Low
Denial of service to other slices resulting in resource exhaustion	• Capping of resources for individual slices • Ring-fencing resources for individual slices	High	Medium
Side Channel attacks across slices extract information about cryptographic keys	• Avoid co-hosting the slices with different levels of sensitivity on the same hardware • Hypervisor hardening	High	Low
Sealing between slices when the UE is attached to several slices	• Security monitoring mechanisms should exist in the network and potentially in UE.	High	Medium
Impersonation attacks against a network slice instance within an operator network	• All virtual functions within a Network Slice instance need to be authenticated and their integrity verified.	Medium	Low

Figure 12. Network Slicing Security – Select Risk Scenarios and Potential Mitigations

Network Slicing Security Opportunities:

- Network slicing enables service differentiation and meeting end user SLAs.
- Enables the isolations of highly-sensitive contexts or applications from non-critical applications.
- Slice-specific SLAs enable a context-aware orchestration and optimization of security virtual functions.
- Slicing could reduce security overhead by eliminating the need for additional layers of authentication.

6.2. Edge Security

The increasingly critical role of the edge in the 5G architecture and use-cases amounts to high adverse impacts if the edge is compromised. When this is combined with the increased threat surface as the edge extends to the end user, the edge becomes an attractive target for cyber-attacks. This is further complicated as the edge hosts security controls such as authentication, authorization and real-time attack detection to provide security controls for other 5G use-cases (as it has been illustrated previously). Security controls should also consider complex and multi-step user handling scenarios, such as in the case of subscriber authentication with a visited network, for a low-latency application. In this case, delay constraints can hinder authenticating against the HSS infeasible, and alternative solution should be considered.

Strong layered security controls must be implemented on the edge to provide adequate protection and availability for the security functions, and any sensitive security contexts that may be stored on the edge, or communicated between the edge and the core. Proper separation of third-party applications and management/network functions would help minimize risks of bi-lateral movement to 5G control plan. Computationally feasible trust platforms could help limiting the attack surface from the user/RAN side.

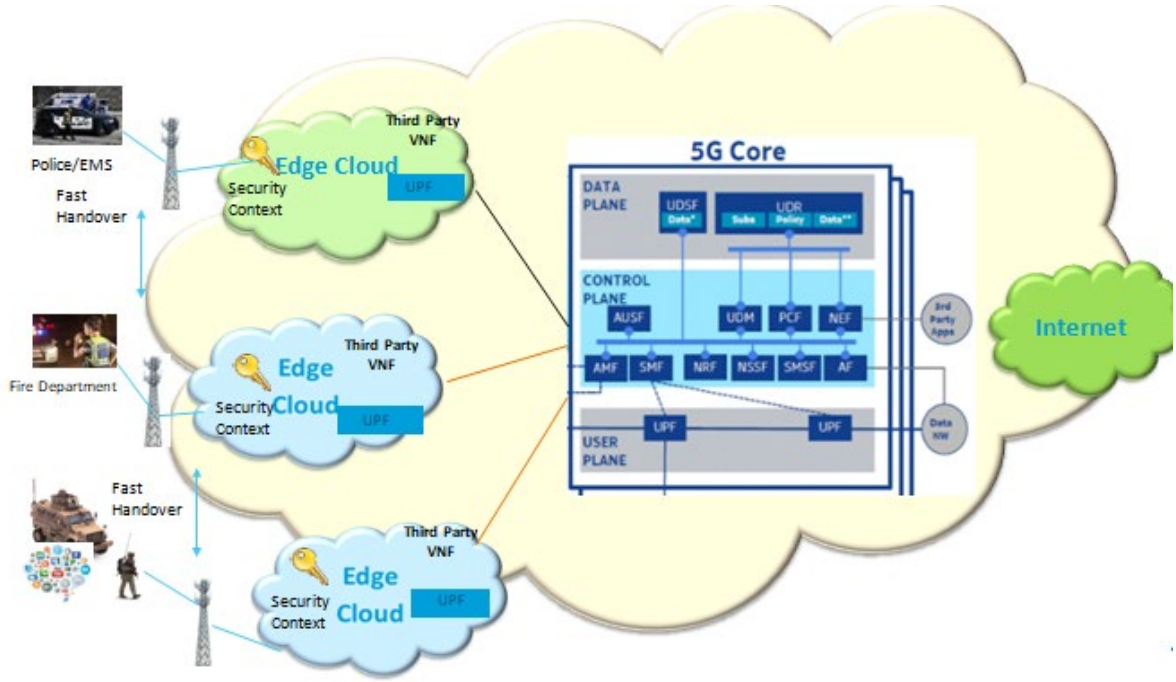

Figure 13. Mobile Edge Security Context

Security Challenges	Potential Mitigation Techniques	Risk Severity	Threat Likelihood
Co-existence of the third party applications with the virtual network functions allow the hackers to infiltrate the platform	• Run both the edge computing applications and the network function(s) in robustly segregated virtual machines. • Higher priority for network functions		
Storage of security context at the edge can lead to malicious spoofing attack	• Apply proper encryption mechanisms for the security context at the edge		
User plane attacks in mobile edge including cache poisoning, cache overwhelming	• Access Control • Hardening Mechanism • Investigate the new security implications		
Spoofing, eavesdropping or data manipulation attack during context transfer	• Encrypted transfer of security context • IDS/IPS for proper monitoring and mitigation,		
Subscriber authentication within the visited networks leads to fraud and lack of control by home operator	• Reuse old security association (SA) while running AKA with the home network and acquiring a new security association. • Timely expiry of temporary security association • Proper authentication between DSS and UE		

High
Medium
Low

Figure 14. Mobile Edge Security - Select Cyber Risk Scenarios and Potential Mitigations

Mobile Edge Security Opportunities:

- Mobile Edge Cloud enable embedding security monitoring at the edge of the network improving security controls against relevant threats.
- Enable application-aware performance optimization.
- Enable reduced latency by way of edge authentication for time-sensitive applications.
- Enable secured and fast data offloading during handover.

6.3. Third Party Security

The continuing increased trend of leveraging commodity modular hardware and software is introducing a multitude of security risks. Example risks include backdoors, dormant malicious code or compromised hardware certificates. Promising solutions that will need to address this on multi-level computationally feasible trust platforms similar to blockchain will enable establishing some security controls over commodity hardware and integrated software. However, capabilities in security monitoring and anomaly detection in the 5G NFV would need to evolve to enable detection/prediction of attacks or malicious incidents.

6.3.1. Supply Chain Security

Supply chain security plays an important role in making sure that the networking components from various vendors and suppliers across the world are properly sourced. Center for Strategic and

International Studies (CSIS) has published a best current practice report around Supply Chain Security (https://www.csis.org/analysis/).

Here are some highlights for best current practice for Supply Chain Security.

- Political and Governance Criteria
    - Trustworthiness of the suppliers
    - Suppliers do not engage in predatory nature of trade practices
    - Acquisition process should not be based only on cost but also environmental social, and governance (ESG), etc.
- Business Practices Assessment Criteria
    - Suppliers demonstrate adherence and observation of accounting
    - Suppliers are financed openly and transparently
    - Best practices in procurement, investment, and contracting
- Cybersecurity Risk Mitigation Criteria
    - Successfully pass independent and credible third-party assessment
    - Suppliers' products and services technologies are designed and built and maintained according to international standards
    - The supplier has a record of addressing and remediating security flaws identified by customers in a reasonable period of time.
- Government Actions to Increase Confidence in Choosing a Supplier
    - Government should have policy and legal tools to assess supplier's risk profile
    - Government and private sector should conduct periodic vulnerability assessment
    - Governments should support the adoption of best security practices for network operators and the implementation of security measures

6.3.2. Open Source / Application Programmable Interface (API) Security

Currently, there are various open-source activities that expedite the deployment of SDN/NFV and 5G. These include Open Networking Foundation (ONF), OPNFV, Open Day Light, Open Network Operating System (ONOS), Open vSwitch (OVS), and the Linux Foundation among others. The operator community and vendor community are collaborating to develop open source that can be scalable and reliable enough to be deployed. Open source has various opportunities such as flexibility and agility, faster time to market, cost effectiveness, long-term cost savings, reducing the vendor lock-in, and better information security. However, open source is also challenged with various issues, namely level of support, intellectual property concerns, lack of documentation and graphical user interfaces (GUIs), extent of customization needed for various use cases. All of these also give rise to security concerns that need to be addressed by the open-source community.

6.3.3. Device / Hardware Security

5G Enables massive expansion of device interactions including V2X, Industry 4.0, Safety Critical Systems (Transport/Rail, Medical, Aviation, etc.). Hardware and device security importance is further highlighted by increasingly growing concerns regarding effective management of supply chain security risk management. Device security and integrity become of paramount importance. Attestation and trusted computing approaches have recently gained significant presence as they provided mechanisms for structured interaction of different types of devices included in the E2E system. TPM/TEE (Trusted Platform Module) is evolving as a service concept to enable trust of elements across the stack of applications.

However, resource and cost limitation will impact how many of the 5G connected devices would be integrated with an attestation platform. As a result, 5G networks will be required to devise approaches to authenticate and authorize untrusted devices and/or increase security monitoring. Moreover, proactive security approaches will enable 5G to anticipate and manage the risk using solutions such as sandboxing or enclaving.

6.4. Data Privacy and Security

Data will be an integrated part of 5G, where the different types of data (including user data, data about the users, system configurations, system logs and monitoring data) will be used to 1) enable core functions and use-cases, and 2) enable automation of decision-making in applications and system management and orchestration.

From a security perspective, several cases should be considered here including classification and proper protection for at-rest and in-transit data. Privacy should be taken into account when designing/configuring the system to ensure only necessary data is collected and stored. Data sharing between subsystems of 5G, and across use-cases and slices should have a structured framework with defined objectives, monitoring and controls.

6.4.1. Satellite Security

Future 5G networks, leveraging software-defined networks, will drive the non-terrestrial solution to be a seamlessly integrated heterogeneous network, between the terrestrial and non-terrestrial networks, and also within the non-terrestrial network across the orbital applications [14].

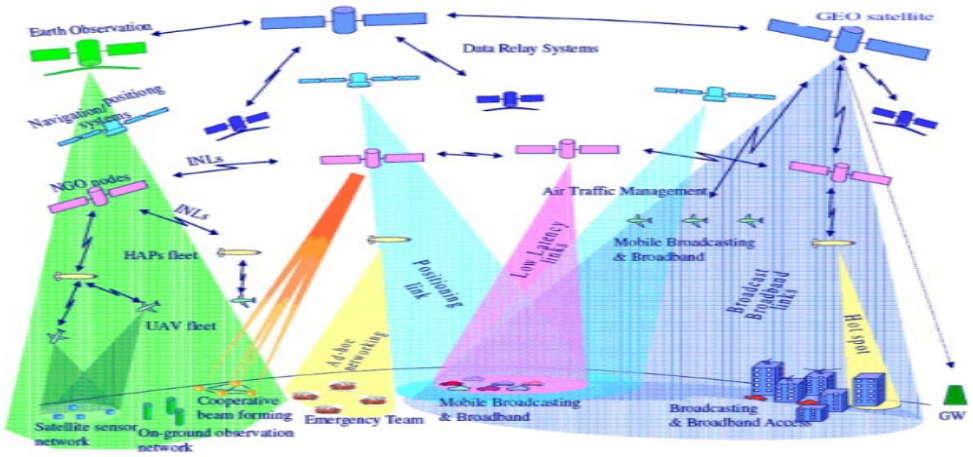

Figure 15. GEO (Geosynchronous Orbit), HEO (Highly Elliptical Orbit), MEO (Medium Earth Orbit), LEO (Low Earth Orbit), and HAP (High Altitude Platforms) [14].

This Beyond 5G integrated network will usher in satellite architectures that are no longer orbital application specific, but integrated networks across all orbital applications (GEO, HEO, MEO, LEO, HAP), and frames the 5G satellite architecture roadmap timeline. Due to the ubiquitous coverage and adaptable beam capacity, there will be no more "stranded/fringe" users [14].

It is clear that the emerging LEO satellite mega-constellations have a high potential to address global connectivity problems in rural areas and densely populated metropolitan centers [15]. The designs of these networks will be challenging as they introduce new constraints in terms of their integration to existing terrestrial networks and the high dynamics of satellites, with traveling speeds of around 27,000 km/hr. In addition to the reliable design of these communication networks towards 6G, the cyber-security of inter-satellite links of these mega-constellations will be another issue that needs to be addressed comprehensively.

Security concerns in satellite communication systems gain attention day by day, and emerging research studies offer new solutions and analyses for different scenarios. The problem is actually far beyond cyber-security challenges that are solely related to the communication environment. The cyber-physical security perspective should be considered as in a holistic manner [16]. For example, maintaining the correct orbit and altitude is one of the critical aspects of reliable communications. The satellites in LEO are exposed to a more substantial gravity impact by the Earth than high-altitude satellites. Therefore, they require an altitude and orbit control (AOC) system to provide stabilization. The AOC system acquires the location data from the GPS receiver and sensors, and it can command maneuver. Maneuver decisions are mainly given by the telemetry, tracking, command, and monitoring system (TTC&M) at the ground station. TTC&M systems sustain operational management of satellites by conveying telemetry and command signals. An attack on telemetry or command signals can lead to interruptions in the communication services of LEO satellites or even collisions of satellites, so the security aspects of these emerging networks are of paramount importance.

6.5. Virtualized Radio Access Network Security

This section describes security opportunities and challenges associated with Virtualized Radio Access Network. Figure 16 shows an example of O-RAN architecture where various RAN functions are dis-

aggregated. The remote radio head and control functions are disaggregated. All the control functions are co-located in the cloud along with other security functions, namely Centralized Unit, Distributed Unit and other Cloud RAN functions.

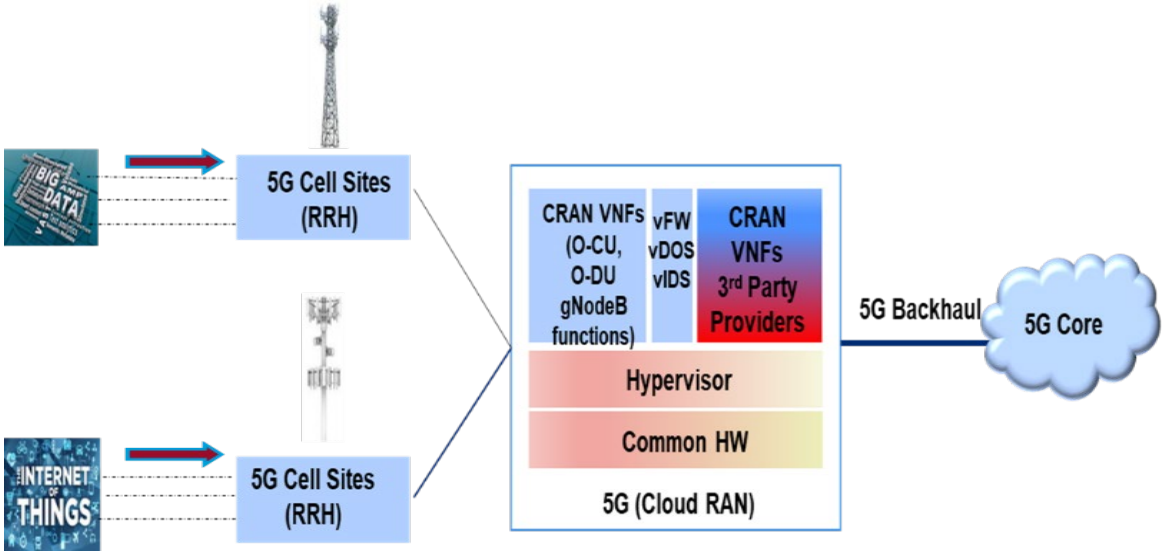

Figure 16. O-RAN Architecture

Security Challenges	Potential Mitigation Techniques	Risk Severity	Threat Likelihood
DDOS (Distributed Denial of Service) attack will result in resource starvation at cRAN Virtual Network Functions due to instantiation of additional vFirewalls	• Intelligent VM resource allocations • Capping of resources • Scale up functionality • Security monitoring at the edge	Medium	Medium
VM (Virtual Machine) manipulation, Data exfiltration due to virtualization	• Hypervisor Separation • Hypervisor Hardening	High	Medium
Programmable and Software RAN will increase the chance of Man-In-The-Middle Attack at the base station	• Traffic monitoring and closed loop orchestration will detect the attacks and mitigate these attacks	High	Medium
Orchestration attack during scaling up and scaling down of VNFs in the cloud RAN	• Deploy detection and mitigation techniques for orchestration and API-based attacks	Medium	Low
Jamming can be launched against control-plane signaling or user-plane data messages	• Deploy DDOS detection, IDS and vFirewall functions • Dynamic Service Chaining • Access Class Barring	Medium	Low

High Medium Low

Figure 17. Cloud RAN Security - Select Cyber Risk Scenarios and Potential Mitigations

Cloud RAN Security Opportunities:

- Programmability and virtualization of RAN will enable adaptive operation to dynamic nature of traffic and multi provider access.
- SoftRAN (cRAN) in 5G networks can enable embedded DDoS detection and mitigation functions.
- Dynamic Radio Resources Scheduling can significantly reduce the risk of jamming attacks targeting mission critical devices.
- Distributed intelligence and correlation of control plane and data plane traffic will enable enhanced security monitoring of traffic.

6.6. Massive MIMO Security

1. Massive MIMO operation is very sensitive to the integrity of the Sounding Reference Signals. A concentrated jamming/attack on these reference signals may disrupt the operation of Massive MIMO systems.
2. The RF energy of Massive MIMO systems can be very directive. If an attacker compromises a Massive MIMO system and maliciously steers a highly focused RF beam at technicians or nearby residential areas, it may pose a health hazard from high energy RF exposure.
3. Electronic attacks through the physical interface.
4. Intrusion detection at the physical layer
5. Reporting and graceful degradation upon electronic attack detection
6. Mechanism to reduce network operation in a jamming environment (The antenna is still operational when jammers are present but whatever you do as mitigation will have an impact on normal system functionality)

6.7. mmWave Security

mmWaves are designed with characteristic narrow beams and small cells with short range, presenting challenges to traditional eavesdropping attacks. Provisioned use of CMOS chips will allow integration of digital functions that could improve security. Supply-chain security remains a risk of concern due to fewer suppliers, i.e., qcom, MediaTek- and the existing possibility to get counterfeit parts or rejected parts.

6.8. Spectrum Security

Security is an implicit dimension of wireless networks. Spectrum allocation can impact security through the administrative decision of access, network type, and frequency amount and location. These issues are explored by examining the proposed Federal Communications Commission's (FCC) 6 GHz allocation for unlicensed use and comparing the network security features of the licensed service 5G versus Wi-Fi, a leading network application for unlicensed spectrum. FCC limitations and challenges to addressing the security of spectrum are discussed. While there is significant policy research in the individual fields of spectrum and security, the intersection of the two fields is relatively new. The

section contributes to bridging of the fields, providing an introductory literature review, and outlining key policy issues.

6.9. Physical Layer Security

In the past years, physical layer security (PLS) has been studied and indicated as a possible way to emancipate networks from classic, complexity based, security approaches. PLS is based on the premise that we can move some of the security core functions down to the physical layer, exploiting both the communication radio channel and the hardware as sources of uniqueness or of entropy. It is usually this second aspect of PLS that is considered in the literature, around the concept of the secrecy capacity and of the secret key generation capacity. As a source of uniqueness, we can leverage PHY by using RF fingerprinting and high precision localization and/or physical unclonable functions for authentication purposes. In essence, as the line-of-sight conditions and the channel quality changes, there is a clear interplay between the use of the CSI for high precision localization (i.e., as an authentication factor) or as the means to distil entropy for use in confidentiality and integrity schemes. This unique setting can only be exploited with enhanced monitoring of the wireless channel and of the context in general.

Overall, PLS can provide information-theoretic security guarantees with lightweight mechanisms (e.g., using Polar or LDPC encoders) as opposed to computationally expensive elliptic curve-based cryptography. At the same time, it is more probable that PLS will be incorporated in hybrid PLS-crypto systems along with symmetric key block ciphers to sustain reasonable communications rates or will act as an extra security layer, complementing other approaches.

In the longer 10-year perspective, the foundational work of formally interconnecting PLS and semantic security can be envisioned by characterizing the predictability / unpredictability of the channel coefficient realizations in the three dimensions of time, frequency and space, as unpredictability is related to indistinguishability, a central concept in crypto proofs.

6.9.1. Physical Layer Security for 6G

A large spectrum of technologies is collectively dubbed as physical layer security (PLS), ranging from wiretap coding, secret key generation (SKG), authentication using physical unclonable functions (PUFs), localization / RF fingerprinting, anomaly detection monitoring the physical layer (PHY) and hardware. Albeit the fact that the fundamental limits of PLS have been largely investigated in the literature, incorporating PLS in future wireless security standards is not a given. Reflecting upon the growing discussion in the community, there is ground to believe that there exist problems in which PLS can offer solutions. At the same time there are non-negligible challenges that will have to be overcome for the practical deployment of PLS in future wireless generations. In further detail, PLS could be employed to provide solutions in the following open issues.

6.9.1.1. Resilience and Robustness Against Active Attacks

Many of the earlier vulnerabilities to jamming and denial of service attacks in earlier generations have been addressed. However, there are now concerns regarding the RAN security for mmWave and mMIMO systems due to vulnerabilities during the beam alignment phase. More generally, the robustness and the resilience of the RAN become much more important with the introduction of cyberphysical systems with different degrees of autonomy. A possible route to circumvent such active

attacks can be provided through stealthy waveform and code design, with early works appearing in this direction.

6.9.1.2. Authentication Using RF Fingerprinting and Hardware Features

Physical unclonable functions (PUFs) and biometrics are currently proposed in many commercial products, albeit there are still open questions regarding the un-clonability of PUFs and their resistance to ML attacks, especially with respect to weak PUFs. For biometrics there are concerns regarding privacy leakage, however it is foreseeable to use them jointly with privacy-preserving technologies, e.g., homomorphic encryption. In terms of implementation, it seems that no universal fuzzy extractor exists, so possibly implementation has to be source specific, although this is still open.

In terms of RF fingerprinting, the need for resistance against jamming, impersonation and injection attacks, arises. As the precision (e.g., with the use of mMIMO) and trustworthiness (e.g., by using multiple sources of fingerprinting) increases, these techniques could be useful in addressing false base station type of attacks, quick authentication in large scale IoT networks and be used as an early or second factor of authentication.

6.9.1.3. Secret Key Generation (SKG) From Wirless Fading Coefficients

SKG relies on the principle that shared randomness between two legitimate users (i.e., reciprocity in the observed channel coefficients during the coherence time of the channel) can be exploited to generate symmetric secret keys. It is a promising solution for a lightweight distributed and scalable key exchange and the principle can be extended to include other sources of shared randomness, e.g., from the hardware or even from a higher-level situation awareness. Added advantages in using SKG include that i) the generated keys are not controlled by any party, potentially providing further privacy and security guarantees; ii) these symmetric keys can be used jointly with block ciphers, e.g., AES-256 towards hybrid systems; iii) the techniques are lightweight and can work is short code lengths which makes them suitable for IoT applications with constrained devices. Most threat models for SKG only account for passive attackers, so accounting jointly for active attacks can allow identify the robustness of these methods in adverse operation environments.

6.9.1.4. Keyless Transmission of Confidential Messages

With the emergence of very narrow beamforming at mmWaves and subTHz, along with visible light communications and free space optics, there is a promising use case for wiretap coding technologies. Recent results on the secrecy performance at finite blocklengths allow understanding the trade-off between secrecy rate, error rate and privacy leakage, which could be pertinent to Quality of Security. Overall, keyless approaches can help resolve other security issues, e.g., information leakage from observing traffic (who exchanges and what amounts of information), etc., that cannot be resolved solely with the use of cryptography in wireless settings. Online learning of the environment, location-based estimation of the channel, etc. are all crucial for the application of these technologies.

6.9.1.5. Anomaly Detection at PHY

Recently, there have been proposals for the identification of anomalies by observing metrics such as transmission and reception times, energy usage, memory usage, etc. These indirect device level metrics can be integrated in distributed anomaly detection at the hardware level.

6.9.1.6. Longer-Term Directions (2030+)

Future generation of wireless are expected to face new security challenges, while benefiting from native AI capabilities towards context (situational) awareness, enabled by whole new set of sensing capabilities in addition to edge and device embedded intelligence. The combination of these enhanced traits can give rise to a new breed of adaptive and context-aware security protocols. In this framework, PLS can fit perfectly for low complexity, low-delay and low-footprint, adaptive, flexible and context aware security schemes, introducing security controls across all layers, for the first time.

6.10. Security Monitoring and Analytics

While it may be effective to detect cyber-attacks quickly and be able to mitigate in a timely manner, stopping the attacks altogether by taking proactive measures is also desirable. This can be achieved by applying AI/ML techniques for anomaly detection, enabling behavior analytics of bad actors through traffic analysis and deep packet inspection, combined with the analysis of past attacks. This approach could improve Zero-Day attacks detection and mitigation. Digital forensics solutions have evolved in the last years to address new challenges imposed by a contextual change.

As 5G enables critical use cases, it should incorporate and enable digital forensic solutions to increase the trustworthiness in the 5G infrastructure from a user-centric perspective. It must be known that, if something happens (malfunction, error or cybercrime), the appropriate technologies will be available to help in the process of identifying the problem and establishing responsibilities.

6.11. Predictive / Proactive Security

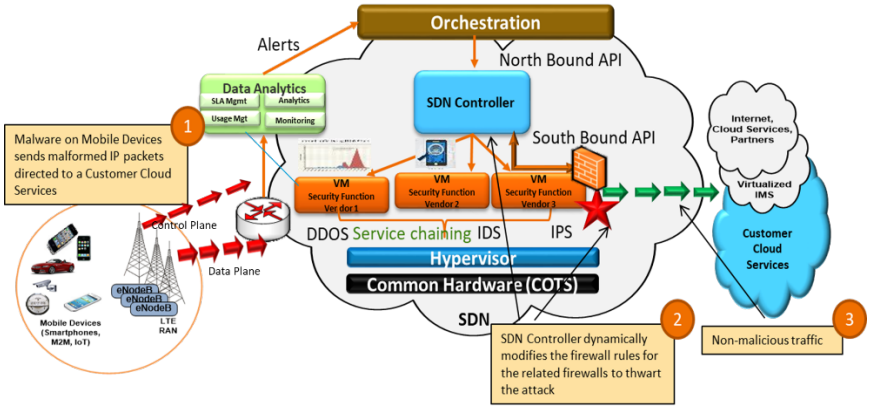

Figure 18. Proactive 5G security

Figure 18 shows an example of how proactive security can be implemented using closed loop automation mechanism by using a combination of Data Analytics, Orchestration, SDN controller and various virtualized security functions.

6.12. Dighital Forensic Solutions for 5G

Digital forensics solutions have evolved in the last years to address new challenges imposed by a contextual change. 5G cannot be an exception. 5G will make possible very risky use cases (e.g., autonomous driving connection) in which, if something happens, can physically affect users. Therefore, offering digital forensic solutions for 5G is not only something natural to the evolution of the context, but a responsibility to the end users and a way to increase the trustworthiness in the 5G infrastructure.

7. SECURITY USE-CASES FOR VARIOUS VERTICALS

This section describes the interaction between security related parameters and various KPIs associated with applications. Different types of applications have different KPIs associated with it. Security affects the KPIs due to authentication and encryption related delays.

7.1. Application Security Requirements

5G will enable emerging applications for various verticals not only for the service providers, but also for other verticals including agriculture, telehealth, first responder, smart grids among others. Various applications can primarily fall into three categories, namely massive bandwidth, massive control, and massive sensing. All of these verticals will need to support various types of applications that have different requirement for various KPIs such as bandwidth, delay, packet loss among others. For example, augmented reality type applications need to support KPIs ranging up to 5 ms. in delay but gigabits per second in throughput. On the other hand, industrial automation type applications may not need that much bandwidth although these types of applications are subjected to stringent delay requirement. Hence, in order to support certain type of applications with desired KPIs various 5G enablers need to be implemented. These enablers include Edge Cloud, Network Slicing, Orchestration among others. However, there are additional security threats associated with each of these enablers that need to be looked into carefully. The following sections describe security and threats associated with a few verticals.

7.2. Critical Infrastructure Systems Security

The critical infrastructure (CI) sectors have greatly benefited from the evolution of Information and Communication Technologies (ICT) over the years. This rapid development of 5G and beyond communication technology has created new verticals for service providers and will be reaching new customers and market spaces. 5G and beyond communication technology research is highly revenue driven. Also, there is a growing need of very high data rate, massive type communication, ultra-reliable low latency and ultra-high availability to meet the need of ever-growing data utilization. This has all started the advent of smart infrastructures, where everything will be connected.

7.2.1. 5G and Critical Infrastructure Amalgamation

Billions of devices will be connecting physical world objects. The Internet of Things (IoT) technology has already been integrated into the CI, making them into the "Smart Infrastructure" to improve performance, decision making, and customer's experience. Some examples are the sensitive military and government facilities, utilities (water, gas, electric, etc.), manufacturing plants, oil and gas rigs, nuclear power stations, and finally, smart cities are starting to rise. The IoT is being adopted overwhelmingly by eHealth, Energy, Transport, Logistics sector and Public Safety to optimize resource utilization, automation of customer monitoring and other facilities. A security and privacy lapse in any of the CI is catastrophic. The 5G and beyond communication technologies that are being developed for CI should have highly resilient security mechanisms. They should not only protect against external cyber-attacks, but also incidents caused by network infrastructure failures.

7.2.2. Smart Grid Use Case

In the Quadrennial Energy Review (QER) second installment of U.S. electricity system, the electrical grids are declared as the most CI, see Figure 19. The electricity grids are transforming due to the development of new energy sources and changing regulation and market structures as they transition into the 21st-century electronic system [1]. Enhancing data connectivity for power grids holds societal, regulatory and economic value. The smart grid is the response to these profound challenges in the way that electricity is generated, distributed, managed and consumed. 5G and beyond communication technology is an important enabler to support new power grid architectures and operational models. Smart grid requires automated controls, higher reliability and better protection mechanisms that can be implemented using 5G technologies [2].

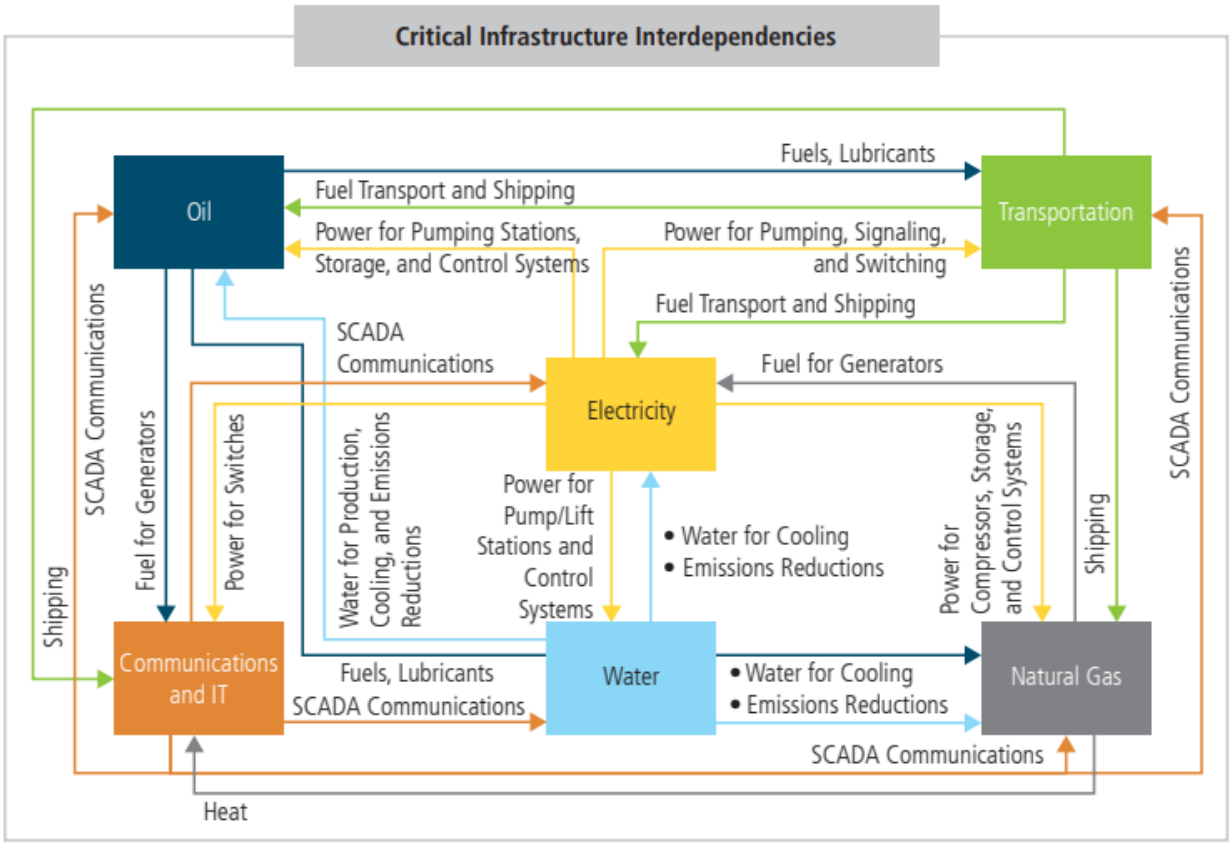

Figure 19. Critical Infrastructure Inter-dependencies [1].

7.2.2.1. U.S. 5G Strategy for National Network and Critical Infrastructure

Cybersecurity and Infrastructure Security Agency (CISA) under U.S. Department of Homeland Security has published a strategy this year to ensure secure and resilient 5G national infrastructure. The CISA director has emphasized addressing potential risks that come with 5G deployment in CI. More so, because it is well known fact that the private sector owns and operates the majority of CI in the U.S., the CISA has outlined 5 strategic initiatives as follows [3]:

1. Strategic Initiative 1: Support 5G policy and standards development by emphasizing security and resilience
2. Strategic Initiative 2: Expand situational awareness of 5G supply chain risks and promote security measures
3. Strategic Initiative 3: Partner with stakeholders to strengthen and secure existing infrastructure to support future 5G deployments
4. Strategic Initiative 4: Encourage innovation in the 5G marketplace to foster trusted 5G vendors
5. Strategic Initiative 5: Analyze potential 5G use cases and share information on identified risk management strategies

7.2.2.2. Threat on Critical Infrastructures

As far back as 2010, it has been reported that the FBI was investigating compromised smart meters in Puerto Rico that were under reporting customer electricity usage. It was believed that it was an inside job [4]. In 2012, a Saudi Aramco facility was under attack by a virus (Shamoon). The virus apparently destroyed or wiped thousands of NT kernel-based versions of MS windows [5]. In 2015, the Ukrainian power grid was hacked using BlackEnergy 3 malware. The attackers targeted power grid industrial control system (ICS) in distribution using advanced persistent threat (APT). Attackers not only caused power outages for more than 200K customers, but the customers were also not able to report the outage as phone lines were also down as part of the attack [6]. In 2017, it has been reported by news outlets that hackers had successfully hacked ICS firmware made by French company Schneider Electric SE generation CI [7]. This ICS is used by nuclear, oil and gas power CI.

The above-mentioned attacks provide current state of cyber security in CI. CISA has a dedicated website (https://us-cert.cisa.gov/ics) that reports advisories and annual reports on CI on regular basis. The annual reports show increase of attacks on CI. CISA work closely with manufacturers and utility companies to ensure better security of their infrastructures.

We would like to mention these WGs that we should be reaching out to:

1. Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council's (CSRIC) is a federal advisory committee made up of members from both the private sector and government. I recommend someone from Security WG should at least participate in these working groups.
    a. Group 2: Managing Security Risk in the Transition to 5G and Working
    b. Group 3: Managing Security Risk in Emerging 5G Implementations to provide recommendations for mitigating risks and identifying best practices within the design, deployment, and operation of 5G networks
2. NRG-5 is a European Unions Horizon funded research and innovation program working to develop Smart Energy-as-a-Service leveraging 5G technologies and contributing in 5G Public Private Partnership (PPP) initiative.

As information technology (IT) and operation technology (OT) borders blur in the age of 5G and beyond communication technology, the threat vectors to CI will increase. What we need to understand is how to integrate and relate the information coming from IT and OT infrastructures or keep them separate as it has been traditionally [8]. This will help us better understand what the threat-resolution process should be in case of a cybersecurity breach. We can't have a one-size-fits-all approach, especially in case of CI.

As more CI comes into the digital realm, where everything is connected and can be monitored remotely, we will be looking at lot more incidents. We need to speed up the work with all stakeholders to build new standards in all areas from device manufacturing to communication network infrastructure protocols. For 5G technology, CIs represent certainly one of the most critical test cases. As each CIs have some unique and large set of diverse security requirements across a variety of applications, we hope that cybersecurity is not a reactive approach, but rather adopts a proactive approach toward the 5G and beyond communication technology for CI.

7.2.3. Emergency and First-Responder Networks Security

This section provides various security-related issues to support Emergency and First Responder Security. Figure 20 shows potential 5G enablers, namely orchestration, network slicing, and edge clouds that can be used to enable emerging applications for the first-responder community. While each of these enablers help provide the desired KPIs to support various first responder applications, there are security issues associated with each of these enablers. Best current practices need to be followed to take care of security threats associated with each of these 5G enablers.

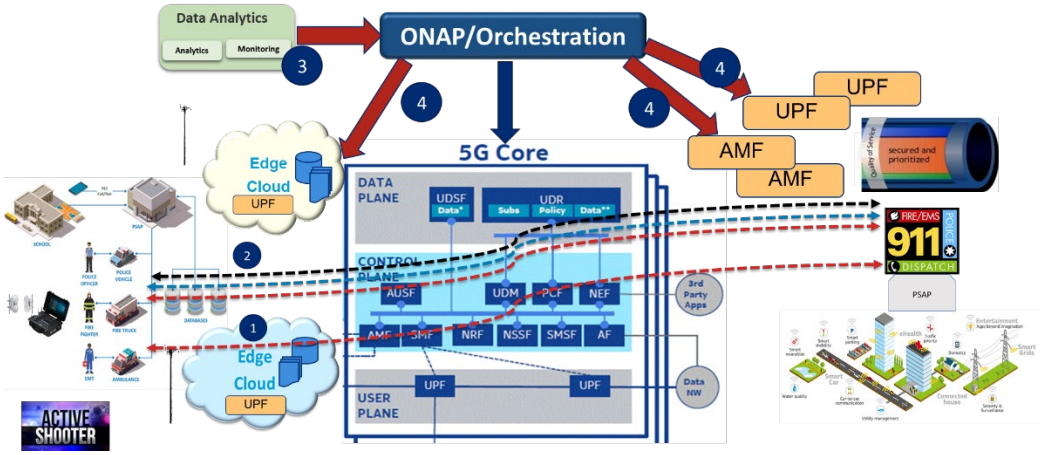

Figure 20. First Responder Use Case on Orchestration

7.2.4. Autonomous Vehicles, V2X Security

An autonomous or automated vehicle is described as using a "combination of sensors, controllers and onboard computers, along with sophisticated software, allowing the vehicle to control at least some driving functions, instead of a human driver". As we move towards increasingly connected and more autonomous vehicles, the complexity of managing threats to those vehicles and their passengers also increases. This field has become an important research trend in the field of intelligent transportation systems and researchers are already focusing on possible automated urban driving scenarios. Automated vehicle technologies allow the transfer of driving functions from a human driver to a computer so that vehicles become connected devices. In the very near future, automated vehicles will also interact directly with each other and with the road infrastructure. However, this environment brings emerging challenges in terms of security and privacy with a combination of physical and digital threats. Thus, it is important to start thinking about the cybersecurity implications of cooperative automated vehicle systems.

7.2.4.1. Cyber Risks and Few Risk Scenarios Exemplified Using Use-Cases Where Possible

Cybersecurity risks are particularly complex for connected devices and vehicles, as they operate across both the physical and digital world, and both consume and create data, while communicating with the surrounding ecosystem. Due to this growing popularity, intelligent transportation networks are hot targets for attackers, who try to exploit the software vulnerabilities of these systems and compromise the security, privacy, and, most importantly, the safety of vehicles and users. In this part, we are ready to

discuss the key challenges of trust, security, and privacy in 5G Vehicle-to-everything (V2X) services. The risks to connected and automated vehicles (CAVs) involve threats related to the vehicle, the CAV ecosystem, and the data collected.

7.2.4.2. Trust Issues in 5G V2X Services: Issues and Attacks

The ubiquitous network connectivity on vehicles creates new possibilities and enlarges the attack surface for hackers to compromise network devices in the 5G V2X architecture. This brings huge concerns to the entities that connect to 5G networks. Moreover, the design flows, misconfigurations, and implementation bugs may cause system failures. In the following, we identify the representative trust attacks in 5G V2X systems.

1. Conflicting Behavior Attacks: Given the fact that a trust is a dynamic event, a malicious entity may have conflicting behaviors, i.e., performing well or badly alternatively, to cover its identity while causing damages. Specifically, an attacker may have time domain inconsistent behaviors, e.g., an attacker may utilize the fact of V2X channel changing to cover its bad behaviors intentionally, which is also named an ON–OFF attack. In addition, the conflicting behaviors of an attacker may happen to two different entity groups, where two groups may have conflicting opinions about the attacker, which can lower the trustworthiness between these two groups. The conflicting attacks subvert trust management by adapting to the dynamic properties of trust in V2X systems.
2. Blackhole Attacks: A blackhole attack, also known as packet, drop attack, is a type of DoS attack, where a malicious entity discards the packets that should be relayed. In multihop routing based V2X services, a malicious entity publicizes its availability of fresh routes regardless of checking its routing table. Moreover, the malicious entity will immediately reply to any request before the response from legitimate system entities.
3. Sybil Attacks: If a malicious entity can forge several fake identities, the Sybil attack occurs. The faked identities can be used to take the blame of bad behaviors, while the real identity can be automatically protected.

7.2.4.3. Security Attacks in 5G V2X: Issues and Attacks

This section presents a systematic view of various security issues in 5G V2X services and particularly identifies some possible existing attacks. 5G V2X services seamlessly connect V2X and 5G communications, which, thus, greatly increase the attack surfaces. In general, the following basic security requirements should be satisfied.

1. Confidentiality: The confidentiality is to prevent the disclosure of information to unauthorized entities so that only intended authorized users can access the data.
2. Authenticity: The authenticity is to confirm the true identity of an entity to distinguish authorized users from unauthorized users in 5G V2X services.
3. Integrity: The integrity is to assure the information transmitted accurate and reliable against any falsification and modification from unauthorized entities.

4. Availability: The availability is to ensure the authorized users can always access the V2X services upon request, and the violation of availability refers to as DoS, which makes the services inaccessible to the users.

In the following section, we review some possible attacks in 5G V2X. Attacks in V2X Communications:

1. Message Forgery: An attacker could fabricate bogus V2X messages or false warnings to mislead the surrounding vehicles, pedestrians, and infrastructure to take wrong actions, which possibly causes some road accidents. To deal with the forgery attacks, V2X entities check the integrity or validity of messages before accepting them.
2. Replay Attacks: An attacker may resend V2X messages previously broadcast by other vehicles, pedestrians, and infrastructure to disrupt the traffic flow, which can cause the receiving vehicles to improperly react to non-existing road conditions.

7.2.4.4. Privacy Issues in 5G V2X Services: Issues and Attacks

In this section, we present a series of privacy issues in 5G V2X services and identify some possible attacks. Privacy Issues in 5G V2X: Due to the pervasive nature of 5G V2X services on roads, it is essential that the users/subscribers have their control over their privacy that may be leaked to the service providers, 5G core, edge servers, or other parties on roads. Here, we provide a list of privacy concerns in 5G V2X architecture.

7.3. AI/ML Security

Given that 5G networks and beyond will support time-critical, safety-of-life applications, a fast, dynamic security architecture is required. Self-driving cars, for example, will require highly secure, low latency networks to operate effectively. Hence, new approaches are required to meet these needs.

Artificial Intelligence (AI) and Machine Learning (ML) capabilities have rapidly evolved over the past decade due to the continued evolution of powerful, low-cost computing resources. While many of the core capabilities of AI/ML have been present for decades, further development of graphics processing units (GPU) for general-purpose computing, along with corresponding software libraries for AI/ML, such as Google's TensorFlow and others, have greatly increased the adoption of AI/ML based systems. Today, applications include pedestrian avoidance, physical security monitoring, high-performance data center networking and many others. However, this field is far from mature as more advanced AI/ML networks, or models, such as Generative Adversarial Network (GAN) have been, and will continue to be, developed to suit next-generation systems.

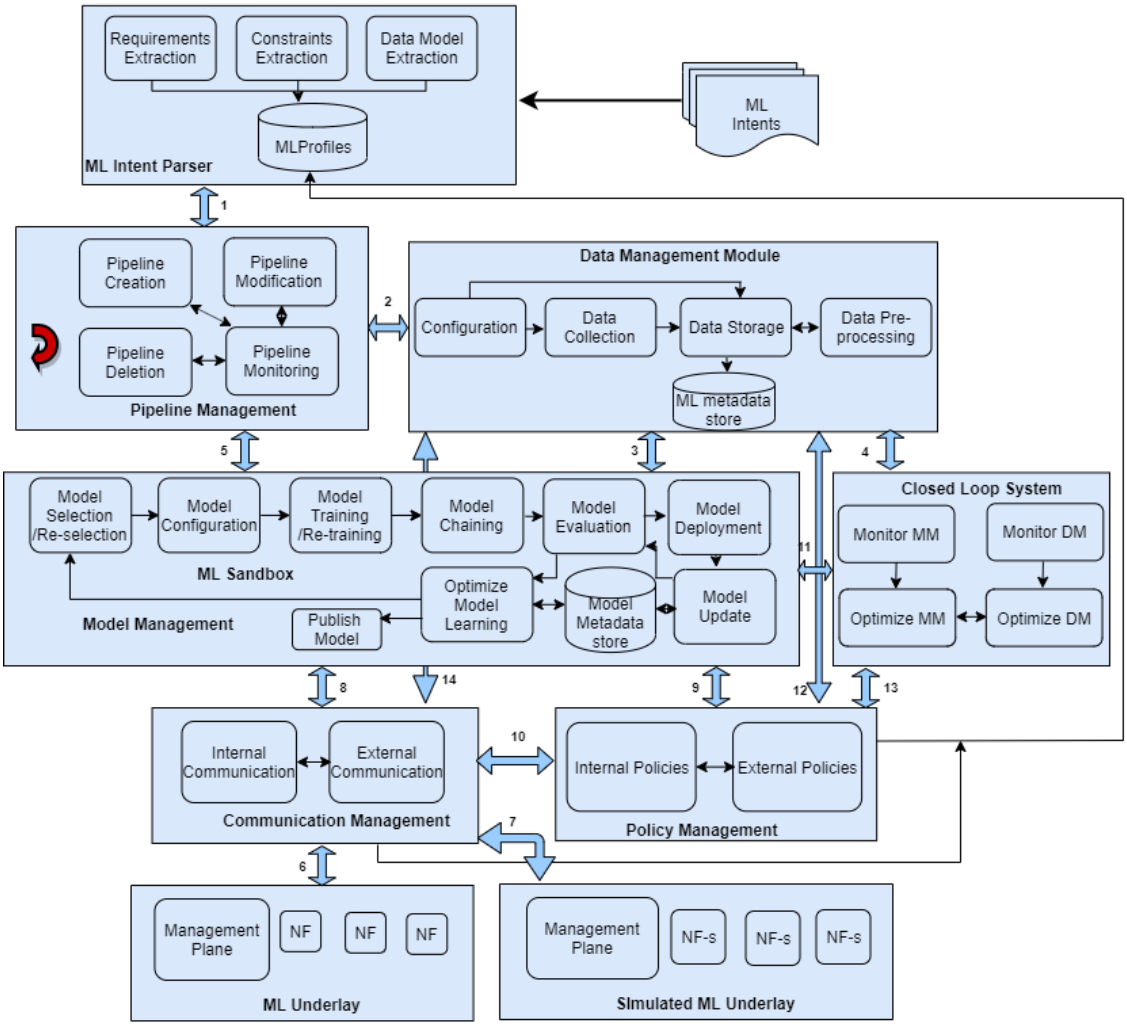

Figure 21. Architecture of the Machine Learning Function Orchestrator [17].

Autonomy is critical for security operation of advanced networks, such as 5G and Future Networks. Consequently, the focus of this document is the security of 5G and Future Networks and how AI/ML can be utilized to secure the network from current and future adversarial attacks. However, AI/ML algorithms alone will not address this problem. The security ecosystem must have a means to both orchestrate the AI/ML security functions. To do so will require an open system to disseminate process and update critical information that includes, but is not limited to, current security threat vectors and levels, changes in AI/ML models and associated parameters. The result will be a dynamic ecosystem where real-time security situational awareness can be achieved.

Given the ability of AI/ML systems to learn and adapt in real-time operations, they will be crucial in protecting against both known (past and current) and unknown (future) threats. The potential of zero-day attacks, or at least the destruction that they can cause, will be minimized with a Dynamic AI/ML Security Ecosystem.

No single AI/ML algorithm or model will be able to achieve this goal. Instead, many specific AI/ML models must be employed to mitigate specific threats that include distributed denial-of-service (DDOS),

jamming and spoofing and others. Future Networks Security is not simply an AI/ML model, but rather, and AI/ML system that can be managed to mitigate many different types of threats. As such, this ecosystem will require management, or orchestration, in order to operate efficiently and effectively against current and future threats.

Ultimately, the goal is to develop the Dynamic AI/ML Ecosystem such that it can support advanced capabilities to secure Future Networks beyond what is capable today. Some of the areas with Security AI/ML will be beneficial includes:

- Enhanced Threat Detection for Network Intrusion Detection and Prevention – Unlike today's intrusion detection and prevention systems, future AI/ML-based systems will be able to learn and adapt in real-time. New models will be developed that can learn from larger sources of data. For example, higher order parameter vectors have the potential to more accurately detect, and remedy threats compared today.
- Threat Model Online Learning – Applications such as self-driving cars, relied on large datasets with associated labels to train their supervised Deep Neural Networks (DNN). Due to rapidly changing cyber security threat profiles, techniques that train in real-time are needed. AI/ML techniques such as GAN and Reinforcement Learning (RL), among other techniques will play an important role in the AI/ML Security Ecosystem.
- Smart Network Controllers – Today, network interface controllers (NIC) process Ethernet packets and pass the data to the network processor. Newer embedded technologies will allow cybersecurity functions to operate at the device level to mitigate threats before they enter the network. For example, SmartNIC devices with AI/ML algorithms can operate on embedded processors and mitigate attacks before they enter the network. New algorithms can be loaded in real-time as the threat profile changes.
- DDOS, Jamming and Spoofing Mitigation – While jamming and spoofing may be considered to be an RF phenomenon only, AI/ML models can be used to detect these threats as the continue to evolve. In doing so, it is possible to develop better situational awareness by recognizing where in the environment that the attacks are taking place.

Some of the core elements of a Dynamic AI/ML Security Ecosystem are listed below:

- Device and Edge Platform Security Functions – Threats that come from the local area that have the potential to become wider network attacks must be mitigated.
- Network Security Functions – Threats to the network that come from the Internet will propagate through Future Networks.
- Supervised and Unsupervised AI/ML Algorithms – There is no single solution to Future Networks security, so all tools must be utilized, and the ecosystem must support many types of AI/ML models.
- Open Interfaces – Interfaces must be specified so that new technologies can be implemented seamlessly and will provide real-time situational awareness.
- Threat Vector Sharing – Share threat vector information in real-time with other models.
- Online Training – Models must train online and update at appropriate intervals.

- Live Updates – Models must be updated in real-time to mitigate security threats and limit the effects.
- Dynamic Model Generation – If the current model cannot mitigate the threat, a new model should be developed in-line to mitigate the threat.
- AI/ML Security Orchestration – Coordination between all elements of the AI/ML ecosystem must take place.

7.4. Interoperability

Open software, such as OpenStack, is a critical component in managing a homogeneous network, such as ones found in data centers and public/private clouds, there will be challenges to implement such an approach in a non-homogenous network that has many disparate components. Issues related to the type of platform, privacy and more will abound. Hence, a single software solution may not be possible. Instead, an Open Systems Architecture (OSA) is needed that will allow network components to connect and interact with each other in order to enhance security of the entire network.

Security OSA would allow network components to communication information in a number of scenarios, such as device to device, device to a security application or device to central controller. This would not require that each network device becomes part of large-scale software program, but rather, each device operates in a distributed fashion with open/published interfaces. In this way, network devices can share real-time security information, AI/ML models and associated parameters, network status updates and more. While the interfaces are open, security functions will be implemented to ensure that information transmitted is both secure and trustworthy. Future research will need to address both of these within the context of an OSA development. Clearly, a 5G network is significantly more complex than that found in a sensor network.

7.5. Industrial Control Systems (ICS): Industrail IOT-Based SCADA

Hacking attacks of factory industrial control systems (ICS) are on the increase. The IIoT is associated with four security concerns:

- Understanding the shift from offline to online infrastructure
- Managing temporal dimensions of security
- Addressing the implementation gap for best practice
- Engaging with infrastructural complexity

7.5.1. Safety and Security

- Confidentiality: (information is made unintelligible to unauthorized individuals, entities, and processes)
- Integrity: (data is protected from modification by a third party, both accidentally and intentionally)
- Authentication: (verification that the data source is the pretended identity)
- Non-repudiation: (ensuring that the sender of a message cannot deny having sent the message).
- Availability: (Ensures that the services of the system is available for legitimate users).

- Privacy: (Ensuring that users' identities are non-identifiable and non-traceable from their behaviors).

7.5.2. Challenges and Opportunities

The 3 main challenges, in general, for solving security issues are [18]:

- Applications operate in highly distributed environments
- Heterogeneous smart objects are used.
- Sensors and actuators are limited in terms of power and computational resources.

Basically, all these devices can be a target for attacks. Such attacks can be directed against critical infrastructure systems, such as power plants and transportation systems, or against household appliances, threatening security and privacy of individuals. Such vulnerabilities include [19]:

- Lack of transport encryption
- Insufficient authentication and authorization
- Insecure web interface
- Insecure software and firmware

The main body of scientific and technical literature has proposed the adoption of security solutions for wireless sensor networks (WSNs) to IoT. However, most security approaches rely on centralized architectures, making their applications in IoT complex due to the large number of objects. Hence, distributed approaches are required to deal with security issues in IoT. Figure 22 discusses various security solutions based on traditional cryptography and emerging technologies such as SDN (Software Defined Networking) and Blockchain.

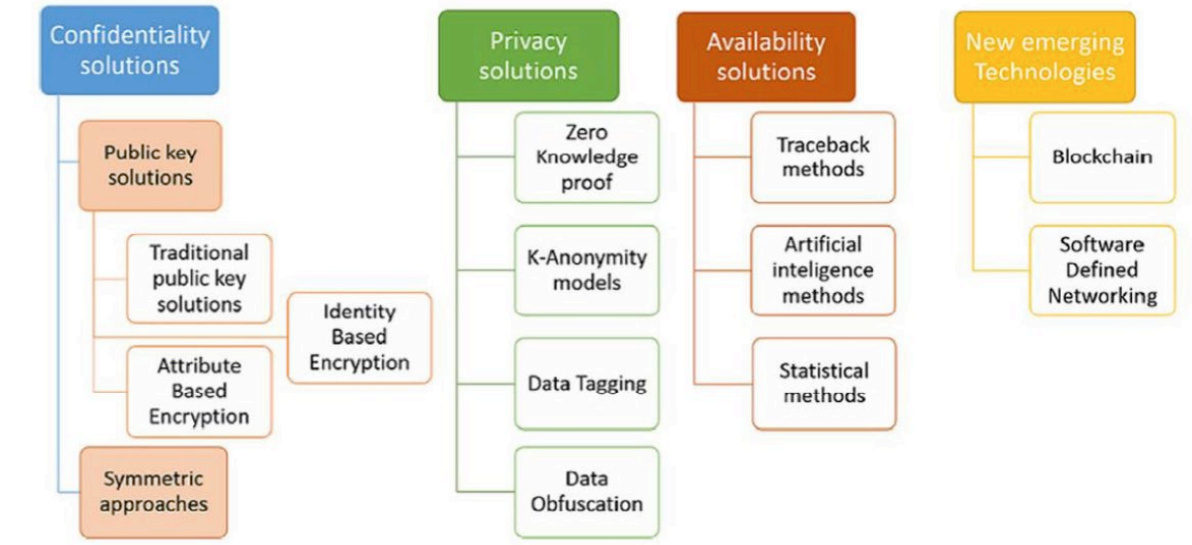

Figure 22. IoT security Solution.

Table 3 summarizes the various threats to the SCADA systems. The physical security of these systems remains a significant issue due to geographical distribution. These systems are expected to run without any interruption, so any patch or upgrade cannot be applied without compromising its productivity.

Moreover, most of the communication happens on the wireless network, which makes it vulnerable to network security attacks [20]. The architecture and design of SCADA systems are available in the form of patents or publications, which make it accessible to hackers. We have also highlighted the vulnerable SCADA component w.r.t. each threat. Sensors and actuators are prone to physical security as they are generally deployed in remote areas. PLC, MTU, and RTUs still uses legacy SCADA software, and are restricted to update.

Table 3. Threats for Scada Systems

Threats
Physical security
Operating System Vulnerabilities
Authentication Vulnerabilities, i.e., Permission, Privileges, and Access controls
Improper authentication, i.e., Unauthorized remote access
Audit and Accountability, i.e., Monitoring and Defenses
Wireless communication network
Legacy SCADA Software Upgrade restriction Public Information

7.5.3. Categories of Risk in the IIoT

Traditional cyber security risks evolve and increase as the IIoT scales up

- **Malware attacks.** The number of malware attacks will increase with the number of internet-connected and software- driven devices, with growing likelihood of cyber-physical impact.

Interconnectedness creates shared and systemic risks

Supply-chain risk. Supply-chain dependence will further increase the risk introduced by specific components. As the density of IIoT devices and connections develops, mapping, monitoring or mitigating supply-chain risks will become increasingly difficult: it may be difficult to tell what is “in” or “out” of the supply chain.

Risks arise from data created by the IIoT

- **Availability of data.** As devices and human decision-making increasingly rely on data. The risk could be through not enough data (for example attacks which stop devices sending telemetry back), or through too much (in the case of denial-of-service attacks which overwhelm a system with more data than it was designed to handle= Botnet IoT).

Risks emerge that are specific to the industrial context

- **Legacy system risk.** Industrial SCADA (Supervisory Control and Data Acquisition) systems often remain in use for 20 years or more – long after original manufacturers have ceased to support them. Legacy systems, which were not designed for IIoT environments and lack security protection, are being increasingly linked to IT and/or IoT networks, creating risk.

Figure 23 shows IIOT based SCADA risk by Threats.

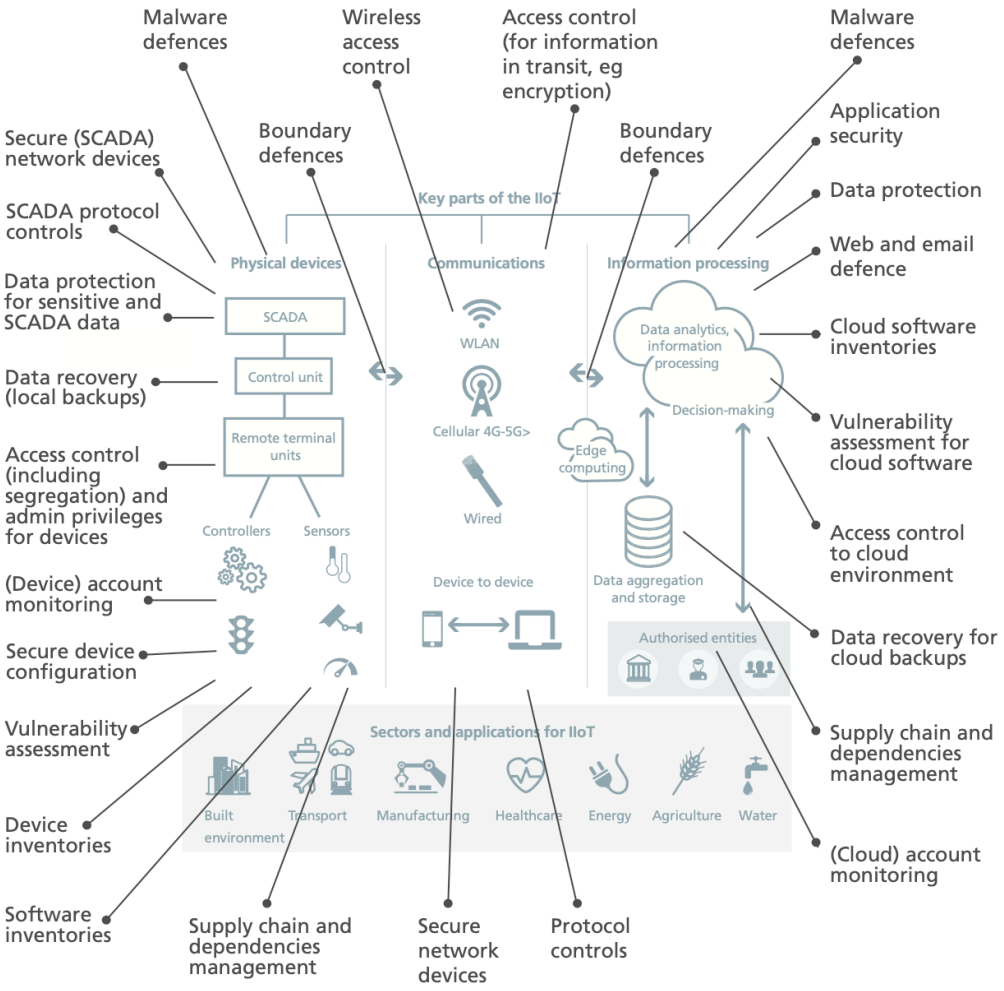

Figure 23. IIoT based Scada Risk by Threats

7.6. Quantum-Ready Security

5G/B5G provides the additional advantages in terms of data rate, spectral efficiency, operation and maintenance, slicing and various other aspects. In access network and RAN it is proposed to use New Radio (NR) with the existing bands which are FR1, FR2 and FR3. Network can be divided into Access

network, transmission network and core network. 5G core is a cloud-based architecture realized with the help of Network Function Virtualization(VNF) and Software Defined Network(SDN). It is designed to support microservices implemented on elastic like cloud backplane. Each services has its own public key for authentication and authorization for any services and access to be offered and to provide secure transactions. In cryptography, key is maintained so that no one can decrypt your data without the key and is based on the principal of prime numbers. Extracting the key requires a complex mathematics which requires large time to perform operation of extraction and in case if the key is large it will take lifetime to get it. In an access network, between UE and RAN, SIM used public key interface for authentications and in case of IoT digital certificates are used. In case of 5G/B5G in addition with the Network Operator and Subscriber, there is a been provision for third party vendor for applications and services in the network. In this case a simple username and its password are considered for the authentication. That 5G used public key infrastructure in most of its authorization and authentication in almost all the sections.

With the advances in the quantum computing, and still following the Moores Law in terms of computation and complexity, the designers of the interface and security issues of using the traditional PKI are having the reservations of securing the operations. A time may reach when quantum computing reaches to its desired level to fail with the present traditional cryptographic techniques because with quantum computing time required for executions shrinks down because order of number of operations becomes less. Also, the 5G infrastructure is going to be there for the longer time as compared to that of previous versions. Hence it is expected to have a safe infrastructure from the quantum computing breaking for the required keys. It is said that as the trends in the development of quantum computing continues, and biggest worry is that quantum computing will break current RSA cryptography and other cryptographic algorithms by 2030. Quantum Algorithms used to crack the RSA are Shor's algorithm and Grover's Algorithm. To make it more secure the size of the key can be increased but will not be of much use because of rapid growth in computing and it will be a matter of time to break such algorithm. Other issue is, though presently these algorithms might not be able to break the key now, but will begin to break it down over the time. So, there is a risk from mischievous actors on network to download the data now and used algorithm afterwards which will be ready to break for the key and get access to the data. This leads to data privacy and security issues open after certain time period. The risk increases over the time as quantum gets more mature and relevant. Due to this, the researchers are searching for the modifications and changes that are required to ensure the advancement in quantum computing does not affect the security issues. A Post Quantum Cryptography (PQC) has been considered with modification in a traditional cryptography for some of these issues to be resolved. Some of the areas under these threats are subscriber and access network security, control plane security. To ensure the 5G systems are safe from quantum Computing Following guidelines are expected to be followed.

1. Carry out data protection inventory and quantum risk assessment.
2. Perform crypto agility analysis and evaluate a hybrid model of traditional and quantum safe.
3. Start building quantum infrastructure for migration in case needed.
4. Evaluate the PQC algorithms
5. Identify the use of QKD for security and privacy

Some of the solutions proposed in these aspects are as follows:

1. Lattice based Cryptography:- In this case it has a public keys, key encapsulations and signature starting in 600–900-byte ranges. Corresponding range for traditional ECC is 32-64 bytes. This offers a better middle way for Post Quantum Computing with efficient running time and average overheads.
2. Hash based Cryptography:- In this it is assumed that for any hash based cryptographic key, there is a limit on number of signatures that can be signed using signed using the corresponding set of private keys, which is for one time use or for "bound in time" signatures. In some cases, Markel signature scheme for quantum protection.
3. Code based cryptography:- These are based on Error Correcting Code (ECC), in which only an authorized designated users knows how to remove the error and recover the desired data. Code based McEliece Public Key Encryption is used in this cryptography.
4. Supersingular Elliptical Curve Isogeny Cryptography:- Here mathematic graph of curve is used to generate the quantum resistance key exchange which can replace the traditional key exchange method. It provides the forward secrecy used in block mass government surveillance.

Quantum Key Distribution (QKD) :- Other option is the use the quantum communication technology to have the encryption and to exchange the key. QKD allows the two entities to establish a secret key between them, using `Photons called as a Quantum information. The quantum information in the form of Photons has unique properties such as it is not possible to make the exact same copy of the quantum information and other is it is not possible to measure or observe the information without introducing the disturbance and modifying it in some detectable method. And due this property of quantum any future advances or computing will not affect it.

As an example, in 5G, SDN orchestration is used to dynamically control the type of encryption deployed for each network slice. 5G provides some encryption of the traffic i.e., Between UE and eNodeB or to secure Gateway. A critical link could be attractive targets for eavesdroppers, hence network operator providing L1 encryption for them. Traditional RSA are vulnerable to the attacks by large scale quantum computers. Possible ways are to use of Quantum resistance algorithms or use of Quantum Key Distribution (QKD). QKD utilizes the quantum states encoded on the photons to agree a key between users with the information theoretic security. QKD is secure against future computational threats, but QRA may be insecure against future quantum hacking algorithms which are not yet discovered. The combination of QRA and QKD can be used to protect the data in network slice. PQR are the software updates whereas QKD is a hardware update.

For the slice the post quantum security is done with QRA. QKD +AES encryption is done . Delivery of CDN is done with QKD. [21] [22] [23] [24]

8. STANDARDIZATION OPPORTUNITIES

As part of cross-team meeting, security working group members are working closely with the Standardization Building Block working group to finalize security standardization opportunities and to proceed with next steps in the process for the specific standards of interest. The working group members within Security working group are considering standards in the area end-to-end security architecture, AI/ML security architecture and optimization, physical layer security and security for SDN/NFV. The working group members plan to submit proposals in the next RRSA meeting scheduled for 2022.

Security working group is collaborating with other working groups such as optimization and is currently coordinating with Standardization working group to bring potential standardization proposals.

9. NEEDS, CHALLENGES, AND ENABLERS AND POTENTIAL SOLUTIONS

Table 4. Proactive Security for 5G-IoT—Needs, Challenges, Enablers, and Potential Solutions

Name	*Current State (2022)*	*3 years (2025)*	*5 years (2027)*	*Future State 10-years (2032)*
Need #1 – Security capabilities in 5G-IoT devices must be improved	There are devices with native security but used for other purposes (e.g., e-payment)	Teams identify potential solutions to provide security using the 5G infrastructure	30% solutions implemented	70% solutions implemented
Challenge(s) for Need 1	Existence of numerous resource-constrained devices, widespread implementation of proprietary protocols, need for backward compatibility			
Possible Solution for Challenge	Teams must analyze if the existent security solutions can be used to build new solutions adapted to the 5G scenarios	Adaptation of open-source framework will reduce the risk of interoperability and backward compatibility issues	Protocols will be optimized so that the resource-constrained devices can utilize a smaller number of resources	Security functions embedded at the design time
Need #2 - Open-source platforms to simulate (security) solutions in 5G	Simulators are mostly focused on low-level communications and network performance rather than on security requirements	Teams are formed by members of very different profiles and various meetings help to define the common requirements of a common simulation platform	Teams promote the information and training in the simulation platform chosen	The simulation platform is widely used by most of the community to test their solutions for 5G
Challenge(s) for Need 2	There are researchers of very different profiles, and a multidisciplinary platform must be provided			
Possible Solution for Challenge	Teams to define a generic open-source platform to be used in 5G by all the experts in different fields cooperatively			
Need #3 – Tools to understand the context of a 5G-IoT environment are required	There are no tools to understand the whole context of a 5G environment	Teams promote cooperation to propose context-aware solutions for 5G-IoT security	10% solutions taken	40% solutions taken
Challenge(s) for Need 3	In order to provide contextual information, it is necessary to be			

Name	*Current State (2022)*	*3 years (2025)*	*5 years (2027)*	*Future State 10-years (2032)*
	able to get a lot of data and be able to process them in a short time. Moreover, human factors should be considered.			
Possible Solution for Challenge	Teams must encourage the definition of solutions to acquire contextual data from IoT devices and combine these with big data analytics in a 5G context.			
Need #4 – Security as a service must be defined to help to provide security to resource-constrained devices and networks	It is a well-established idea that part of the advanced functions that a device needs could be provided by the 5G infrastructure.	Teams analyze the problem and propose solutions accepted by representative stakeholders	Solutions are proposed and some prototypes are implemented	Some commercial solutions available for 5G end users
Challenge(s) for Need 4	Improve the technologies at the edge to provide security services, definition of truss mechanisms for 5G infrastructures including resource-constrained devices			
Possible Solution for Challenge	Teams analyze this need considering the main technologies that that will bring the core closer to users (e.g., MEC, Fog computing)			
Need #5 – Privacy-aware solutions for 5G-IoT must be considered	Works for specific use-cases related to 5G, but the general vision is missing. The users are exposed if their devices contribute their contextual data to the security of the 5G infrastructure. Privacy-aware digital forensics is a current open challenge for IoT-Forensics.	Teams analyze the repercussion of privacy in 5G-IoT security and digital forensics and propose solutions	Standards proposed	20% Standards adopted

Name	*Current State (2022)*	*3 years (2025)*	*5 years (2027)*	*Future State 10-years (2032)*
Challenge(s) for Need 5	To ensure that the stakeholders understand their rights and responsibilities. To ensure the success of some solutions depends on the user's cooperation in order to work (e.g., related to the digital forensic topic). It must be analyzed how 5G-IoT solutions will be affected by the General Data Protection Regulation (GDPR).			
Possible Solution for Challenge	Teams propose techniques to inform users of different technical profiles about the management of their data in a clear way. Analysis of security solutions proposed from the point of view of privacy.			

Table 5. AI/ML Security – Needs, Challenges, Enablers and Potential Solutions

Name	*Current State (2022)*	*3 years (2025)*	*5 years (2027)*	*Future State 10-years (2032)*
Need #1 The architecture for the Dynamic AI/ML Security Ecosystem needs to be developed	Currently, there is no architecture that describes how to implement AI/ML into 5G and Beyond systems.	Identify teams and architectural trade-offs. Examine potential technologies.	Define architecture and requirements for a subset of market verticals or use-cases.	Implement fuller set of requirements for more verticals.
Challenge(s) for Need #1	There are many stakeholders and methods to implement AI/ML, though less for security			

Possible Solution for Challenge	Specify requirements and interfaces that allows vendors to plug in solutions.			
Need #2 Open systems and interfaces are needed for the Ecosystem	In order to support many vendor technologies, and allow for plug-and-play operation, open interfaces are needed for the AI/ML Security Ecosystem.	Organize teams to develop standard interfaces and requirements. Determine an approach to developing open-source AI/ML Security interface software.	Complete first version of open interface specification and develop initial version of open-source software.	Evolve the requirements and update open-source software.
Challenge(s) for Need #2	Current AI/ML models are standalone and not easily modified.			
Possible Solution for Challenge	By defining standard interfaces, vendors can develop modular technologies that can be easily implemented, which accelerates innovation an implementation.			
Need #3 An AI/ML orchestration framework is needed	The AI/ML Security Ecosystem is complex with many parts, higher-layer technology is needed to manage and support the Ecosystem.	Organize teams to define a limited set of functionalities and define orchestration architecture. Work with open-source community to develop software.	Finalize limited orchestration architecture and associated open-source software.	Evolve orchestration architecture and open-source software.

Table 6. Digital Forensics Solutions for 5G Environments—Needs, Challenges, and Enablers and Potential Solutions

Name	*Current State (2022)*	*3 years (2025)*	*5 years (2027)*	*Future State 10-years (2032)*
Need #1 Common framework to express digital forensics requirements in 5G	Relevant works in specific areas (e.g., IoT-forensics, vehicle-forensics and SDN-forensics) without considering the whole complexity of 5G networks	Teams define proactive digital forensic solutions for 5G	Tools and formal procedures to acquire and analyze 5G artifacts are proposed	The definitions and procedures proposed by the teams are accepted by a representative community of stakeholders

Name	*Current State (2022)*	*3 years (2025)*	*5 years (2027)*	*Future State 10-years (2032)*
Challenge(s) for Need 1	Determine the liability of actions and discourage misbehavior, greater heterogeneity of devices (and services), digital forensics and privacy trade-offs			
Possible Solution for Challenge	Teams to design specialized information-retrieval tools, definition of common formats to share relevant data and to extract information, promote cooperative approaches			
Need #2 There are not enough cooperative approaches for digital forensics	Some approaches define witnesses (vehicular or IoT) in order to provide digital evidence to help digital investigation, but these approaches are not directly applicable to 5G	Teams define the mechanisms to enable the digital cooperation using 5G infrastructure	Prototypes are developed and tested	The new platforms for cooperative digital forensics can be used and are accepted by the community
Challenge(s) for Need 2	The devices at the edge must be prepared (proactive) to provide relevant information about the context, some of these devices can be resource constrained, and there are no tools specific for IoT environments			
Possible Solution for Challenge	Teams define specific working groups to work in this issue, define tools and mechanisms for the cooperation			
Need #3 Privacy-aware digital forensics for 5G-IoT	Privacy-aware digital forensics is a current open challenge for IoT-Forensics	Teams analyze the repercussion of privacy in 5G-IoT security and digital forensics and propose solutions	Standards proposed	20% Standards adopted

Name	*Current State (2022)*	*3 years (2025)*	*5 years (2027)*	*Future State 10-years (2032)*
Challenge(s) for Need 3	The user must be aware of the life cycle of their data. It must be analyzed how 5G-IoT solutions will be affected by the General Data Protection Regulation (GDPR).			
Possible Solution for Challenge	Teams to analyze possible privacy problems in this early phase and propose solutions and countermeasures. Look for a closer approach to the user and propose solutions for their training.			

10. CONCLUSIONS AND RECOMMENDATIONS

10.1. Summary of Conclusions

In this document, the IEEE Future Network Initiative's Security working group has identified the security requirements in a stepwise manner, focusing on a 3-, 5- and 10-year timeline on a priority basis. The security working group has explained some of the key security pillars for 5G and beyond networks. Security implications for some of the key use cases have also been cited. Since security requirements permeate all other working groups and have an inter-dependency, this document also highlights the need for interaction with other working groups as part of cross-team interaction. This document also underscores the importance of gap analysis by looking into security work being done in other SDOs and how the IEEE Future Network Initiative can add value and complement the existing security work. Some of the future state security work that can be carried out as part of short-term and mid-term planning are also described. Finally, this document outlines five key topics as part of needs, challenges associated with the needs and solutions and provide details for 3-, 5- and 10-year horizon. Key recommendations have been laid out as part of next steps.

10.2. Working Group Recommendations

The working group recommends the following set of activities:

- Perform an in-depth gap analysis with current industry standards with respect to security:
    - Utilize the IEEE RRSA vehicle for proposed new standards:
        - IoT connectivity: identity and access management, tamper proofing, etc.
        - Encryption and certificate management to support seamless QoE
        - Guidelines on SDN/NFV security controls orchestration/optimization

    - Collaborate with ongoing standardization efforts
- Enable studies (research, verification) via established 5G testbeds
    - NSF, WINLAB, 5G-Lab, etc.
    - Publicly accessible and available for researchers (academic, industry)
- Publications to inform/guide/socialize 5G security directions/focus areas (informed by the roadmap). These include:
    - Publications—whitepapers, journal special issue, tech-focus (work-in-progress).
    - Focus areas—virtualization security, threat taxonomy, security trade-offs, decentralized identity, security-based prioritization, slicing security, resilience, privacy-preserving algorithms, etc.
- Collaborations with ONF, ORAN, Linux Foundation to develop an open-source security framework
- Engagement, education and socialization—conferences, panels, webinars, world forum

10.2.1. Future Work

The INGR security roadmap working group will continue working to advance the roadmap to take into consideration recent advancements in technology, the threat landscape and evolution of use-cases and applications. The working group also recognizes opportunities for security standardization, where the WG will seek to propose a few standards in conjunction with other working groups where necessary. It is also part of the WG focus to further develop an in-depth discussion of several topics in the next editions including data sharing and privacy, satellite security, identity and access management, application security KPI/SLAs and to include additional use-cases and applications. To support the WG objectives, they will participate actively in presenting and sharing their work in conferences, workshops, webinars and podcasts as available. While involved in those venues, the working group members will be collecting input from interested communities including, industry, standards and academia. In summary:

- Systematically include 5G specific applicable risk scenarios, security challenges and opportunities to each of the topics covered topics.
- Further develop the next edition to provide more in-depth coverage of data sharing and privacy, satellite communication, physical layer security, identity and access management, application security KPI/SLA, etc.
- Include more use-cases and applications with a description of end-to-end security requirements, risk scenarios and risk mitigation scenarios.
- Propose a few security standards through existing IEEE standardization vehicles in collaboration with other working groups.
- Formalize high-level generic security reference architecture as a generalization of existing detailed models.
- Develop detailed recommendations for a subset of the roadmap topics.

Actively present the WG work in academic, industrial and professional venues, events and publications.

11. CONTRIBUTOR BIOS

Dr. Ashutosh Dutta is currently Senior Wireless Communication Systems Research Scientist and JHU/APL Sabbatical Fellow at Johns Hopkins University Applied Physics Labs (JHU/APL), USA. Most recently he served as Principal Member of Technical Staff at AT&T Labs in Middletown, New Jersey. His career, spanning more than 30 years, includes Director of Technology Security and Lead Member of Technical Staff at AT&T, CTO of Wireless at a Cybersecurity company NIKSUN, Inc., Senior Scientist in Telcordia Research, Director of Central Research Facility at Columbia University, adjunct faculty at NJIT, and Computer Engineer with TATA Motors. He has more than 90 conference and journal publications, three book chapters, and 30 issued patents. Ashutosh is co-author of the book, titled, "Mobility Protocols and Handover Optimization: Design, Evaluation and Application" published by IEEE and John & Wiley that has recently been translated into Chinese Language. Ashutosh served as the chair for IEEE Princeton / Central Jersey Section, Industry Relation Chair for Region 1 and MGA, Pre-University Coordinator for IEEE MGA and vice chair of Education Society Chapter of PCJS. He co-founded the IEEE STEM conference (ISEC) and helped to implement EPICS (Engineering Projects in Community Service) projects in several high schools. Ashutosh currently serves as the Director of Industry Outreach for IEEE Communications Society and is the founding co-chair for IEEE 5G initiative. He also serves as IEEE Communications Society's Distinguished Lecturer for 2017-2020. Ashutosh serves as the general co-chair for the premier IEEE 5G World Forum. He was recipient of the prestigious 2009 IEEE MGA Leadership award and 2010 IEEE-USA professional leadership award. Ashutosh obtained his BS in Electrical Engineering from NIT Rourkela, India, MS in Computer Science from NJIT, and Ph.D. in Electrical Engineering from Columbia University under the supervision of Prof. Henning Schulzrinne. Ashutosh is a senior member of IEEE and ACM.

Dr. Eman Hammad is a cybersecurity professional & interdisciplinary professional focusing on trustworthy & resilient complex systems and emerging technologies. She obtained her PhD in Electrical & Computer Engineering from the University of Toronto. Eman combines practical experience and theoretical research to shape her vision for resilient-by-design solutions in the connected world. She is the director of the innovations in Systems Trust & Resilience (iSTAR) lab. Eman's work has been published in more than 50 papers, and was recognized with merit awards (best paper award, best poster award) and has been featured on multiple outlets. Most recently, she was honored as one of Canada's Top 20 Women in Cybersecurity. Eman is a senior IEEE member currently serving as Toronto ComSoc chair, and the co-chair of the IEEE 5G Security working group for the International Network Generations Roadmap (INGR). She delivered numerous invited talks in academic and industrial conferences, chaired and co-chaired several conferences and workshops, and participated in several panels. She serves on the advisory board of several initiatives. Eman is an active advocate for diversity and inclusion in STEM and Cybersecurity. Her service has been recognized by IEEE exceptional, chapter achievement, and exemplary service awards.

Dr. Michael A. Enright is the CEO/President of Quantum Dimension, Inc. and has 30 years of experience in Cybersecurity, Artificial Intelligence and Machine Learning, Embedded Computing, Quantum Computing, RF Communication and more. For the 16 years at Quantum Dimension, Michael has led engineers in the company's technology developments, which includes AI/ML, RF communication and navigation using advanced embedded DSP/GPU/FPGA technologies. He has been an Adjunct Professor in the Electrical Engineering Department at USC, where he taught both undergraduate and graduate courses in image and signal processing, digital communications, and wireless communication systems design.

Michael has a Ph.D. in Electrical Engineering from the University of Southern California (USC), an M.S. in Electrical Engineering from the Illinois Institute of Technology, an M.S. in Mechanical Engineering from the University of Missouri-Columbia and a B.S. in Aeronautical and Astronautical Engineering from the University of Illinois at Champaign-Urbana. Michael Senior Member of the IEEE.

Arsenia (Ersi) Chorti

Arsenia (Ersi) Chorti is a Professor at the École Nationale Supérieure de l'Électronique et de ses Applications (ENSEA), Joint Head of the Information, Communications and Imaging (ICI) Group of the ETIS Lab UMR 8051 and a Visiting Scholar at Princeton and Essex Universities. Her research spans the areas of wireless communications and wireless systems security for 5G and 6G, with a particular focus on physical layer security. Current research topics include : context aware security, multi-factor authentication protocols, 5G / 6G and IoT, anomaly detection, machine learning for communications, new multiple access techniques and scheduling. She is a Senior IEEE Member, member of the Steering Committee of the Competitive Pole Systematic and of the PhD Thesis GdR ISIS Award Committee in France. Since October 2021 she is chairing the IEEE Focus Group on Physical Layer Security.

Sanjay S Pawar, Ph.D

Dr. Sanjay S Pawar, done his Masters M.Tech (Communication) and Ph.D (Networking) from Department of EE, Indian Institute of Technology, Bombay (IITB), He presently working as a Independent consultant and Principal at BCREC, and has total 30 years of experience teaching/research/ and Consultancy. The area of Interest is 5G Wireless Networks, Software Define Networks, Small Cell, Fiber Optics Networks, Machine and Deep Learning in Communications. He has total around 50 papers in International Journals and Conference to his credits, out of which 4 papers/projects have received best paper awards in reputed IEEE Conference as a Co-Author with his research scholars and funding to carry out further research. Sanjay mentored several research proposal in the area of Machine Learning from Department of Science and Technology, Govt. of India. One student has completed the Ph.D in the area IPV6 Low Power Personnel Area Network (6LoWPAN), He has supervised 4 Ph.D thesis some of them sponsored by Department of Electronics and Information Technology, GoI, and other sponsoring agencies. He has also supervised several Masters thesis He has given various talks in the conferences, invited talks, Corporates etc in the area of 5G/B5G Edge Networks, AIML, etc.

Julia Urbina

Julia begins her career in Information Security from her research work to graduate in Engineering in Electronics and Communications from UDLAP Mexico, with the title of Intrusion Detection Systems in Computer Networks. She continued his training at the Center for Electronics and Telecommunications (CETEC) – ITESM Mexico, to obtain the degree of Master of Science - Electronic Engineering - with a specialty in Prediction Algorithms for Handover Shot Detection for mobile networks, and Doctorate in Technologies of Information with a specialty in identification of Botnets based on DNS, where she was decorated as IEEE Honor Member – Etta Kappa Nu (HKN) in 2013. Since 2017, Julia founded CyberIIoT, where scientific consulting services are offered, such as: security architecture design, risk analysis and cybersecurity maturity of Organizations and training for personnel from higher education institutions, governments, financial institutions, the industrial and operational branch (OT/SCADA). As of 2020, she was appointed Executive Director 5G security and Industry 4.0 for IoTSI LATAM, with the purpose of raising awareness about IoT security with the use of the IoT security Framework for private 5G networks in companies and industry. Starting 2021, she is appointed President of the Communications Society Chapter of the IEEE Puebla Section, where one of her objectives is to promote information cybersecurity in wireless mobile communications and 5G networks.

Gunes Karabulut Kurt

Gunes Karabulut Kurt received the B.S. degree with high honors in electronics and electrical engineering from the Bogazici University, Istanbul, Turkey, in 2000 and the M.A.Sc. and the Ph.D. degrees in electrical engineering from the University of Ottawa, ON, Canada, in 2002 and 2006, respectively. From 2000 to 2005, she was a Research Assistant with the CASP Group, University of Ottawa. Between 2005 and 2006, she was with TenXc Wireless, Canada. From 2006 to 2008, Dr. Karabulut Kurt was with Edgewater Computer Systems Inc., Canada. From 2008 to 2010, she was with Turkcell Research and Development Applied Research and Technology, Istanbul. Between 2010 and 2021, she was with Istanbul Technical University. She is currently an Associate Professor of Electrical Engineering at Polytechnique Montréal, Montreal, QC, Canada. She is a Marie Curie Fellow and has received the Turkish Academy of Sciences Outstanding Young Scientist (TÜBA-GEBIP) Award in 2019. In addition, she is an adjunct research professor at Carleton University. She is also currently serving as an Associate Technical Editor (ATE) of the *IEEE Communications Magazine* and a member of the IEEE WCNC Steering Board. She is the chair of the IEEE special interest group entitled "Satellite Mega-constellations: Communications and Networking". Her current research interests include space information networks, satellite networking, wireless network coding, wireless security, space security, and wireless testbeds.

Ahmad Raza Cheema received his Ph.D. degree in Electrical and Computer Engineering from Lakehead University, Thunder Bay, ON, Canada, in 2021. He also has a Master's degree in information security from the University of Bradford, UK. He is currently working as a Technical Advisor with Shared Service Canada a Federal Government Department. He is also an experienced information security and IT trainer having trained 1K+ professionals from the military, government, industry, banks, and academia. His research interests include wireless communication, network security, informational and operational technology cyber security, Internet of Things, and digital forensics. He is a member of IEEE 5G and Beyond Technology Roadmap Security working group. He was secretary IEEE Communication Society Islamabad Section, Pakistan. He has also been elected to the grade of Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

12. REFERENCES

[1] *3gpp, "The mobile Boradbacnd Standard." www.3gpp.org. Accessed: June 30, 2020.*

[2] *IEEE, "IEEE Future Networks Enabling 5G and Beyond." https://futurenetworks.ieee.org/. Accessed: June 30, 2020.*

[3] *ngmn, "Next Generation Mobile Networks Alliance." www.ngmn.org. Accessed: June 30, 2020.*

[4] *5G Lab Germany, "5G Lab Germany." https://5glab.de//. Accessed: June 30, 2020.*

[5] *Ericsson, "A look at key innovation areas of 3GPP Rel-17." https://www.ericsson.com/en/blog/2019/12/3gpp-rel-17. Accessed: June 30, 2020.*

[6] *J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3gpp 5g networks," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 170–195, 2019.*

[7] *ETSI, "ETSI Network Functions Virtualisation (NFV) Specifications." https://www.etsi.org/deliver/etsi gs/NFV-SEC/001 099/. Accessed: August 9, 2020.*

[8] *5G PPP, "5G Eenablers For Network and System Security and Resilience." https://5g-ppp.eu/5g-ensure/. Accessed: August 9, 2020.*

[9] *Ashotush Dutta, Eman Hammad, "5G Security Challenges and Opportunities, a System View", IEEE 5G World Forum, virtual, 10-12 September 2020.*

[10] *Z. Tian, Y. Sun, S. Su, M. Li, X. Du, and M. Guizani, "Automated attack and defense framework for 5g security on physical and logical layers," arXiv preprint arXiv:1902.04009, 2019.*

[11] *GSMA, "Mobile Telecommunications Security Threat Landscape." https://www.gsma.com/security/wp-content/uploads/2019/03/GSMASecurity-Threat-Landscape-31.1.19.pdf. Accessed: June 30, 2020.*

[12] *National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity", 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed: January 20, 2021.*

[13] *National Institute of Standards and Technology (NIST), "Guide for Conducting Risk Assessments", 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. Accessed: January 20, 2021.*

[14] *IEEE INGR, "INGR Roadmap – Satellite Working Group 1st Edition," 2020.*

[15] *C. Daehnick, I. Klinghoffer, B. Maritz, and B. Wiseman, "Large LEO satellite constellations: Will it be different this time," McKinsey & Company, https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/large-leo-satellite-constellations-wil.*

[16] *O. Topal, M.O. Demir, Z. Liang, A. Pusane, G. Dartmann, G. Asheid, and G. Karabulut Kurt, "A Physical Layer Security Framework for Cognitive Cyber Physical Systems," IEEE Wireless Communications Magazine, vol. 27, no. 4, Aug. 2020.*

[17] *International Telecommunication Union, FG ML5G Technical Specification, "FG ML5G Technical Specification "Requirements, architecture, and design for machine learning function orchestrator", July 2020.*

[18] Saad Albishi, Ben Soh, Azmat Ullah, Fahad Algarni (2017) Challenges and Solutions for Applications and Technologies in the Internet of Things. Procedia Computer Science 124: 608-614.

[19] Bruno B, Rodrigo S, Cláudio T, Sean CA (2017) A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications 84: 25-37.

[20] Krushna Chandra Mahapatra and S Magesh. Analysis of vulnerabilities in the protocols used in scada systems. International Journal of Advanced Research in Computer Engineering & Technology, 4(3), 2015.

[21] *T. Charles Clancy, Robert McGwier and Lindong Chen, " Tutorial, Post Quantum Cryptography and 5G Security" WiSec 19, May 15-17, Miami, Florida 2019.*

[22] *Edward D Amoroso, " Securing Emerging 5G Global Networks and Mobile Infrastructures", TagCyber, Quantum Exchange.*

[23] *Mervin Ivezic, "The quantum Computing threat to Cyber Security and 5G", https://cyberkinetic.com/quantum-computing/quantum-threat-5g-security/.*

[24] *Vicor Lovic, "Quantum Key Distribution, Advantages, Challenges and Policies" Cambridge Journal of Science and Policy, Vol. 1. Issue 2, 2020, pp 1-10.*

13. ACRONYMS/ABBREVIATIONS

Term	Definition
SDO	Standards-Developing Organisations
3GPP	3rd Generation Partnership Project
NR	New Radio
IMSI	The international mobile subscriber identity is a number that uniquely identifies every user of a cellular network. It is stored as a 64-bit field and is sent by the mobile device to the network.
GTT	Global title translation is the SS7 equivalent to IP routing
OTT	Over-The-Top operators provide services over the internet supported by broadband internet access service (BIAS) providers
BIAS	Broadband Internet Access Service provider
NRM	Network Resource Model
NSMF	Network Slice Management Function
NSSI	network slice subnet instance (NSSI)
NSI	Network Slice Instance
CSC	Communication Service Customer (CSC): Uses communication services. B2C, B2B or B2B2X
CSP	Communication Service Provider (CSP): Provides communication services Designs, builds, and operates its communication services.
NOP	Network Operator (NOP): Provides network services. Designs, builds, and operates its networks to offer such services.
VISP	Virtualization Infrastructure Service Provider (VISP): Provides virtualized infrastructure services. Designs, builds, and operates its virtualization infrastructure(s). Virtualization Infrastructure Service Providers may also offer their virtualized infrastructure services to other types of customers including to Communication Service Providers directly, i.e., without going through the Network Operator.
DCSP	Data Center Service Provider (DCSP): Provides data center services. Designs, builds, and operates its data centers.
NEP	Network Equipment Provider (NEP): Supplies network equipment. For sake of simplicity, VNF Supplier is considered here as a type of Network Equipment Provider.
NFVI Supplier	NFVI Supplier: Supplies network function virtualization infrastructure to its customers.
GSMA	GSMA represents the mobile operators worldwide, including 750+ operators ~400 companies in the broader mobile ecosystem (handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors).
MPS	Multimedia Priority Service (MPS)

cRAN	cloud based radio access networks (cRAN)
cMTC	Critical MTC
NR light	NR Light communication is based on NR building blocks, such as numerology and SSB bandwidth, but complemented with enhancements to meet the new requirements such as reduced complexity and lower UE power consumption.[5]
ITS	intelligent transportation systems (ITS)
gNB/gNodeB	5G Base Station
NG-RAN	Next generation RAN
EPC	Evolved Packet Core (EPC) is a framework for providing converged voice and data on a 4G Long-Term Evolution (LTE) network
PLMN	Public land mobile network
IPX	P exchange or (IPX) is a telecommunications interconnection model for the exchange of IP based traffic between customers of separate mobile and fixed operators as well as other types of service provider (such as ISP), via IP based Network-to-Network Interface. IPX is developed by the GSM Association.
AMF	Access & Mobility Management Function, example 5G NF
SMF	Session Management Function, example 5G NF
UPF	User Plane Function, example 5G NF
DU	Distributed Unit of gNodeB, example 5G NF
CU	Central Unit of gNodeB, example 5G NF
ARPF	Authentication credential Repository and Processing Function, example 5G NF
UDM	Unified Data Management, example 5G NF
SUCI	Subscription concealed identifier
SUPI	Subscription Permanent Identifier
GUTI	Globally Unique Temporary Identifier
SEPP	Security Edge Protection Proxy
SEAF	Security Anchor Function
AUSF	Authentication Server Function
SIDF	Subscription Identifier De concealment Functionality
AKA	Authorization and Key Agreement
OSS/BSS	Operations Support System / Business Support System
Term	Definition

IEEE ANTITRUST STATEMENT

Generally speaking, most of the world prohibits agreements and certain other activities that unreasonably restrain trade. The IEEE Future Networks Initiative follows the Anti-trust and Competition policy set forth by the IEEE Standards Association (IEEE-SA). That policy can be found at: https://standards.ieee.org/wp-content/uploads/2022/02/antitrust.pdf