International Network Generations Roadmap (INGR)

An IEEE 5G and Beyond Technology Roadmap

Security

1st Edition

FutureNetworks.ieee.org/Roadmap

International Network Generations Roadmap (INGR)

Chapters:

- Applications and Services
- Edge Automation Platform
- Hardware
- Massive MIMO
- Satellite
- Standardization Building Blocks
- Millimeter Wave and Signal Processing
- Security
- Testbed

White Papers:

Available 1st Quarter 2020

- Artificial Intelligence & Machine Learning
- Deployment
- Energy Efficiency
- Optics
- Systems Optimization

Download the entire document at

FutureNetworks.ieee.org/Roadmap

An exclusive benefit for subscribers to the

IEEE Future Networks Initiative.

Table of Contents

Tables

Figures

ABSTRACT

It is imperative to embed security functions from the very beginning while the 5G architecture is being defined and standardized. Security requirements need to overlay and permeate through different layers of the 5G systems—namely physical layer, network layer, and application layer—as well as different parts of an E2E 5G network. Since the 5G network is fundamentally based on Software Defined Networks (SDN) and Network Functions Virtualization (NFV), many of the challenges and opportunities applicable to SDN/NFV networks would also be applicable to 5G networks, as well. In that respect, 5G security needs to pay attention to additional security requirements, such as SDN controller security, hypervisor security, orchestrator security, cloud security, API security, supply chain security, data security, open source security, as well as security under multi-tenancy settings while keeping in mind the existing security threats. At the same time, one needs to take advantage of the security opportunities provided by the 5G networks. This roadmap document addresses the challenges and opportunities associated with the security for 5G networks and discusses the security roadmap for Future Networks.

Key words:

SDN/NFV, Network Slicing, Cloud RAN, Mobile Edge Cloud, Edge Detection

SECURITY

1. INTRODUCTION

1.1. WORKING GROUP VISION

The Big Picture for Security

Security and privacy must be the integral part that mature and evolve alongside technology and its applications. As these technologies are integrated into our daily life operations, such as smart home, 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 would have been standardized, and 30% deployment would have been completed. In 5 years, 5G would 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 (e.g., global service provider). 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 would be able to withstand sophisticated cyber-attacks and continue to be available and functioning with minimal impact by providing resilient and flexible services.

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 end-points 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 than the exception. End-devices will be plug and play in a heterogeneous ecosystem.

3, 5, and 10 years' 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 pervasive. 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.

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, as human identify human similarly smart object 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 end-points are people, systems, or simply two applications on a single machine). Security will 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 an 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.

1.2. 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.

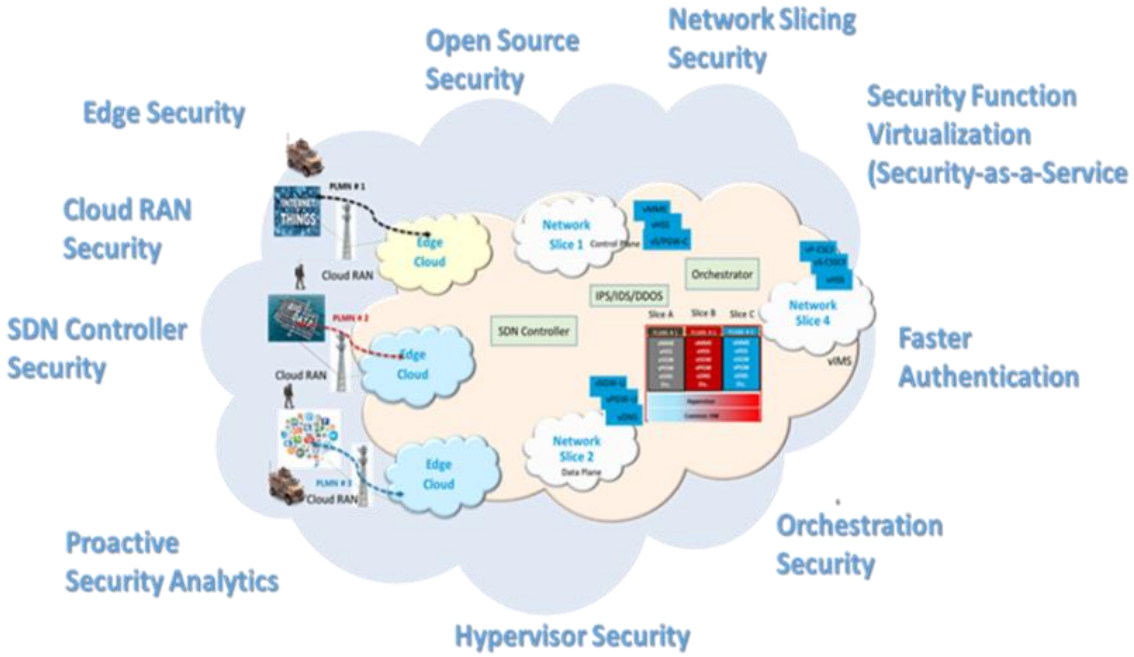


Figure 1. Various Security Pillars for 5G Networks

While 5G security needs to take in to account all these pillars described in Figure 1, we will explain only a few of these in this document as follows.

- Management and Orchestration Security:
  - Virtualization/softwarization security
  - Optimization/orchestration security
  - SDN security
  - Network slicing security
- Edge Security
- Third Party Security:
  - Supply chain security
  - Open source/application programming interface (API) security
- Data Security and Privacy
- Security Monitoring and Analytics:
  - Proactive security for 5G/IoT
  - Digital forensics solutions for 5G environments

This first edition of the security roadmap implicitly considers a hierarchal architecture model. Future editions should discuss that architecture in more detail specifically following an OSI-type model with multi-layer security paradigm. The future edition should also align 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).

Security is a foundational by-design enabling component of all 5G verticals/applications/services. 5G is an enabler of exciting use cases that will transform the way humanity lives, works, and engages with its environment. 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, as follows:

- 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 backbone 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 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 context need to be stored in the edge cloud to reduce the 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 that a 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, counter-measures for API-based security vulnerabilities will need to be explored.

- Entertainment services—Because the current 4G cannot economically support such bandwidth-hungry applications, 5G could support interactive mobile games. Sporting events could utilize effective and efficient usage of spectrum and leverage new broadcast capabilities, such as 4D.

  Security Concerns—Man in the middle attack, 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, the ability to hold mobile devices to accident victims coupled with pressure sensitivity from doctors and health specialists would provide valuable opportunities. 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.

Future editions of this framework would include deep-dives on the following:

- Gaps in standards
- 5G security architecture and requirements (including cyber resilience 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
- Alignment with NIST Cyber Security Framework
- Data sharing platforms and privacy

1.3. LINKAGES AND STAKEHOLDERS

The Security Roadmap is a horizontal 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) would 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 bake off 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 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.

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

Forum	Forum
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
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. TODAY'S LANDSCAPE

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 user 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 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 needs to be collected, stored or shared. There needs to be a defined framework for secure and governed data sharing.
- **Network Slicing Security—**Scenarios that would introduce some required cross functionality between slices, such as if a user equipment (UE) can consume services from multiple slices need

to be further examined from a cyber-risk perspective, and proper controls to be placed to ensure the mitigation of any risks when this function is enabled.

Gaps in Standards (or other enablers)

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

- 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.

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.

3. FUTURE STATE

3.1. MANAGEMENT/ORCHESTRATION SECURITY

3.1.1. 5G 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. Attacker can then use hypervisor privilege to install kernel root kit in VNF's operating system (OS) and thereby controls and modifies 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. Use of software vulnerability management procedure 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 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.

3.1.2. Optimization/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 will provision virtual network functions (VNFs) based on the network condition and network intelligence. For example, in case of overload or security attacks, 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 orchestrator can help to scale out by instantiating additional VNFs. As the attack subsides, orchestrator can scale down the VNFs. While orchestrator adds the flexibility, there is also potential vulnerability for the orchestration. An attacker can use legitimate access to the orchestrator and manipulates 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; automated system or configuration auditing. Deployment of security monitoring system can detect the compromised VNF separation, any kind of anomaly in the system or provide 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.

3.1.3. 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 mis-configuration and source code vulnerability that need 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 attack 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.

3.1.4. 5G 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 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.

3.2. 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 will 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.

3.3. THIRD PARTY SECURITY

3.4. SUPPLY CHAIN 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 will need to address this on multiple levels—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 attacks or malicious incidents detection/prediction.

3.4.1. OPEN SOURCE / 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. Operator community and vendor community are collaborating to develop open source that can be scalable and reliable enough to be deployed. While 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), level of support, 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.

3.5. DATA SECURITY AND PRIVACY

Data will be an integrated part of 5G, where the different types of date (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:

- Data classification must direct the application of security controls to ensure proper data protection at-rest and in-transit.
- System and functions logs and events will be continuously collected to enable AI/ML-based algorithm (e.g., orchestration, security DPI, etc.). Such data must be communicated securely to minimize the risk of Man-in-The-Middle (MiTM) attacks.
- Privacy should be taken into account when designing the system functionality to ensure only necessary data is collected and stored. Data sharing between subsystems of 5G, and across use-cases and slices should be have a structured framework with defined objectives, monitoring and controls.

3.6. Proactive Security for 5G-IoT

While it is effective to detect the attacks quickly and be able to mitigate in a timely manner, stopping the attacks altogether by taking proactive measures is very much desirable. This can be achieved by applying AI/ML techniques for anomaly detection. This would enable looking at pattern of the traffic, performing behavior analytics of bad actors, and the analysis of past attacks. This will assist in improving Zero-Day attacks detection and mitigation. Applicability of AI/ML is going to play a major role to provide proactive security analytics instead of looking at the attack after it has taken place.

3.7. Digital Forensics Solutions for 5G Environments

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. 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.

4. Needs, Challenges, and Enablers and Potential Solutions

4.1. Proactive Security for 5G-IoT

4.1.1. Needs, Challenges, and Potential Solutions Narrative

The term “proactive security” means that the environment will be prepared to be secure (and reactive) by design. This is very difficult to guarantee in general terms, and even more so in 5G-IoT environments, where are resource-constrained devices, or critical ones in which applying automatic countermeasures can be a problem. However, proactive security will be the only way to stop advanced attacks effectively in their initial stages of spread. Considering that IoT devices are highly exposed, having been used for various DDoS attacks, providing these devices with proactive security mechanisms can be a turning point for security in 5G infrastructures. In order to address these issues, it will be necessary to define security mechanisms that use native security or provide security services through the 5G infrastructure. All this taking into account the fact that it will be fundamental to know and interpret the context around the area affected by an attack quickly and efficiently to provide adequate countermeasures.

4.1.2. ROADMAP TIMELINE CHART

Table 1. Proactive Security for 5G-IoT—Needs, Challenges, and Enablers and Potential Solutions

Name	*Current State (2019)*	*3 years (2022)*	*5 years (2024)*	*Future State 10-years (2029)*
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 less amount 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 than on security requirements	Teams are formed by members of very different profile 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 the 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 able to get a lot of data and be able to process them in a short time. Moreover, human factors should be considered.			

Name	*Current State (2019)*	*3 years (2022)*	*5 years (2024)*	*Future State 10-years (2029)*
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 with 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 (2019)*	*3 years (2022)*	*5 years (2024)*	*Future State 10-years (2029)*
Challenge(s) for Need 5	To ensure that the stakeholders understand their rights and responsibilities. Ensure the successful of some solutions that 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 upcoming 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			

4.2. DIGITAL FORENSICS SOLUTIONS FOR 5G ENVIRONMENTS

4.2.1. NEEDS, CHALLENGES, AND POTENTIAL SOLUTIONS NARRATIVE

Digital forensics solutions have evolved in the last years to address new challenges imposed by a contextual change. 5G cannot not 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. 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.

4.2.2. ROADMAP TIMELINE CHART

Table 2. Digital Forensics Solutions for 5G Environments—Needs, Challenges, and Enablers and Potential Solutions

Name	*Current State (2019)*	*3 years (2022)*	*5 years (2024)*	*Future State 10-years (2029)*
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
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			

Name	*Current State (2019)*	*3 years (2022)*	*5 years (2024)*	*Future State 10-years (2029)*
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
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 upcoming 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.			

4.3. CROSS-PLATFORM SECURITY

4.3.1. NEEDS, CHALLENGES, AND POTENTIAL SOLUTIONS NARRATIVE

Cross-platform attacks are attacks designed to pivot between multiple platforms taking advantage of the convergence of technologies and the lack of synergy between security mechanisms to avoid the propagation to other technologies in the same infrastructure. For example, in *Software Defined Networks* (SDN) through API exploitation, an attacker can gain control of SDN controllers and then jump between different networks. Even some devices connected to the 5G infrastructure can have malware waiting for the connection to jump to another environment until reach a target. Cross-layer attacks can be very difficult to predict and identify, because each technology/orchestration manager uses its own security controls that have not been designed to efficiently cooperate or to understand complex contexts such as 5G. Therefore, the attackers can exploit the vulnerabilities in a particular technology to gain control over other critical components in the 5G architecture. As the technology map of 5G is highly complex, it is a perfect breeding ground for cross-layer attacks.

4.3.2. ROADMAP TIMELINE CHART

Table 3. Cross-Platform Security—Needs, Challenges, and Enablers and Potential Solutions

Name	*Current State (2019)*	*3 years (2022)*	*5 years (2024)*	*Future State 10-years (2029)*
Need #1 Cross-platform attacks definition and specific cases for 5G	Specific examples can be found in the literature, but there is no a common definition for this problem.	Define new methodologies to identify cross-platform attacks and to stop them.	Some prototypes are developed for SDN. Also, some solutions can be developed for end-user devices.	Standards can be proposed in order to ensure common steps to be implemented by the community.
Challenge(s) for Need 1	Multiple technologies must be analyzed and the vectors for the cross-platform attacks must be defined.			
Possible Solution for Challenge	Different experts must cooperate in order to face the problem cooperatively, defining a common framework for the analysis.			
Need #2 Promote the interoperability between existent intrusion detection systems and event managers to identify cross-platform attacks	Multiple solutions for intrusion detection, some of these use big data, also security information and event management (SIEMs) are widely known although the configuration of these systems is not easy. Also threat intelligence platforms are used to identify common threats.	Threat intelligence is widely used to classify attacks. Some solutions are developed to take advantage of these systems to recognize attacks.	Different 5G platforms can use intermediary platforms to identify cross-platform attacks and the role of the platform in the attack (source, intermediary, and target).	Cross-platform attacks can be classified by intrusion detection systems deployed in 5G ecosystems. SIEMs are nourish with relevant data about the incidents.
Challenge(s) for Need 2	Current solutions are not fully interoperable, and the configuration is generally complex. Furthermore, these are prepared for specific environments, the traceability of the attack is difficult nor impossible when the network is used only as intermediary and the intrusion detection systems are not prepared to identify the attack.			

Name	*Current State (2019)*	*3 years (2022)*	*5 years (2024)*	*Future State 10-years (2029)*
Possible Solution for Challenge	Develop open source solutions supported by a motivated community. Common languages must be proposed for classification, based on existent SIEMs.			
Need #3 Define new classifications for attacks considering the cross-platform nature	Vulnerabilities can be classified by common vulnerabilities and exposures (CVE) numbering authorities (CNAs) using CVEs.	New vulnerabilities are identified and classified, but the cross-platform perspective is missing.	The classification of new vulnerabilities is improved to consider additional factors.	The classification of new vulnerabilities also consider threat intelligence parameters for detection.
Challenge(s) for Need 3	The classification is specific for attacks on particular platforms, systems and services.			
Possible Solution for Challenge	The vulnerabilities should also include the potential effect that can have, depending on the type of device that can be connected to the vulnerable service or platform.			

4.4. 5G SECURITY TESTING

4.4.1. NEEDS, CHALLENGES, AND POTENTIAL SOLUTIONS NARRATIVE

Nowadays there are multiple open source simulators with modules to test networks. In the context of 5G technologies, some users in the community are developing useful modules to test specific communication protocols but these modules may not be interoperable. Security testers must rely on modules developed by contributors that are focused on different topics, without a clear synergy in the development of 5G modules for open source simulators. Prior the development of large scale 5G networks, security must be tested in multiple scenarios, with the ability to simulate all the potential 5G technologies together. This must be available not only to vendors, but also to researchers and other contributors.

4.4.2. ROADMAP TIMELINE CHART

Table 4. Security Testing—Needs, Challenges, and Enablers and Potential Solutions

Name	*Current State (2019)*	*3 years (2022)*	*5 years (2024)*	*Future State 10-years (2029)*
Need #1 5G security must be tested but the experts in security perhaps are not experts in 5G specific technologies.	Proprietary simulators such as Nets include 5G modules. Open source simulators depends on the community that develops modules for different versions not necessarily interoperable (e.g. OMNET++, NS2, NS3)	New 5G modules are developed, but security researchers cannot build (yet) their solutions on the specific simulators.	Some modules to test 5G security are developed to specific technologies and environments.	New modules and specific solutions are developed to test security in simulators.
Challenge(s) for Need 1	Develop new modules for 5G that are interoperable in open source simulators.			
Possible Solution for Challenge	Choose a network simulator as a reference and incentive the development of interoperable modules.			

4.5. TRUSTED COMPUTING

4.5.1. NEEDS, CHALLENGES, AND POTENTIAL SOLUTIONS NARRATIVE

Trusted computing brings new opportunities to develop security solutions using the notion of *core-of-trust*. This ensures the integrity of a device or platform starting on the booting process and maintaining the integrity measurements during the whole lifecycle of the system. This implies the use of anti-tampering hardware that is embedded in the devices with security capabilities that are under its potential. A clear example of evolution is the Trusted Platform Module (TPM) chip that initially was used in personal computers and servers and nowadays can be used in cars (v.2.0). Similar solutions are used in smartphones (e.g., Titan M) and even in IoT devices. Also there are hybrid solutions built on the basis of secure hardware adapted to cloud environments. Some processors have the feature of trusted execution that also helps to develop the notion of trusted computing. The 5G ecosystem should take advantage of these features, but also be able to define methodologies to ensure the integrity of the trusted computing solutions themselves.

4.5.2. ROADMAP TIMELINE CHART

Table 5. Trusted Computing—Needs, Challenges, and Enablers and Potential Solutions

Name	*Current State (2019)*	*3 years (2022)*	*5 years (2024)*	*Future State 10-years (2029)*
Need #1 analysis of trusted computing solutions for 5G	There are multiple analysis that are very general, on trusted computing.	Analysis about trusted computing in 5G use cases will be available.	More analysis about other new devices	Some methodologies for trusted computing in 5G emerged
Challenge(s) for Need 1	Widespread number of technologies and trusted computing cannot be applied to all.			
Possible Solution for Challenge	Classify the potential devices that cannot be benefited by the trusted computing solutions and propose alternatives.			
Need #2 Classification of trusted computing devices and environments	Propose some methods to identify and classify the devices based on its trusted computing capabilities.			
Challenge(s) for Need 2	Some devices will depend on the vendor.			
Possible Solution for Challenge	Encourage the participation of vendors on this initiative			
Need #3 Develop trusted computing aware solutions	Identify potential scenarios for 5G use cases			
Challenge(s) for Need 3	Large number of technologies and scenarios			
Possible Solution for Challenge	Select a subset of devices and scenarios based on potential cooperative vendors.			

5. CONCLUSIONS AND RECOMMENDATIONS

5.1. SUMMARY OF CONCLUSIONS

In this document, the IEEE Future Network Initiative's Security working group has identified the security requirements in a step-wise 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.

5.2. 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/optimisation
  - Collaborate with ongoing standardization efforts
- Enable studies (research, verification) via established 5G test-beds
  - 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

6. CONTRIBUTORS

Ashutosh Dutta	John Hopkins University
Ana Nieto	University of Malaga
Eman Hammad	University of Toronto, PwC
Ahmad Cheema	Lakehead University
Ahmed Limam	
Anton Kaska	
Colby Harper	Pathfinder Wireless
DJ Shyy	MITRE
David R Varner	CenturyLink, Inc.
Gerhard Fettweis	TU Dresden
Harold Tepper	IEEE
Jay Goswami	Ericsson
John Lester	MITRE
Julia Urbina-Pineda	IEEE
Linda Wilson	IEEE
Marc Emmelmann	
Mischa Dohler	King's College London
Nigel Jefferies	Huawei Technologies
Omneya Issa	Communications Research Centre – Canada
Rajakumar Arul	Amrita School of Engineering – Bengaluru
Sanjay S Pawar	Usha Mittal Institute Of Technology
Sivaramakrishnan	

7. REFERENCES

[1] “Next Generation Mobile Networks Alliance”, www.ngmn.org

[2] “IEEE Future Networks”, www.futurenetworks.ieee.org

[3] “The 3rd Generation Partnership Project (3GPP)”, www.3gpp.org

[4] “NIST Cybersecurity Framework 1.1”, https://www.nist.gov/cyberframework.

[5] “5G Lab | Next Generation Network”, https://5glab.de/

[6] ETSI NFV Security - https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/

8. ACRONYMS/ABBREVIATIONS

Term	Definition
1G-4G	First Generation to Fourth Generation
3GPP	Third Generation Partnership Project
5G	Fifth Generation
ACK/NAK	Acknowledgment/negative acknowledgment
AI	Artificial intelligence
API	Application programming interface
B2B	Business to business
B2C	Business to consumer
BS	Base station
BSS	Business support system
CAPEX	Capital expenditure
CDMA	Code division multiple access
CN	Core network
CNAs	CVE numbering authorities
COTS	Commercial off-the-shelf
CP	Control plane
CVE	Common vulnerabilities and exposures
C/U	Control plane/User plane
D2D	Device to device
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed denial of service
DevOps	Development and information technology operations
DFT-s-OFDM	Discrete Fourier transform spread orthogonal frequency division multiplexing
DL	Downlink
DOD	Department of Defense
EAP	Edge automation platform
eMBB	Enhanced mobile broadband
eNB	Evolved node B
EPC	Evolved packet core
ETSI	European Telecommunications Standards Institute
FDD	Frequency-division duplex

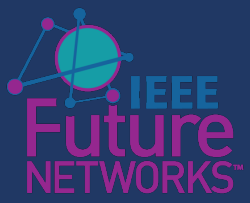
Term	Definition
FDMA	Frequency division multiple access
GDPR	General Data Protection Regulation
GHz	Gigahertz
GSMA	GSM (Groupe Speciale Mobile) Association
GUIs	Graphical user interfaces
HIR	Heterogeneous Integration Roadmap
IDS	Intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP multi-media subsystem
IoT	Internet of things
IP	Internet protocol
IRDS	International Roadmap for Devices and Systems
ISG	Industrial specification group
ISP	Internet service provider
ITS	Intelligent transport system
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
KPI	Key performance indicator
LAA	Licensed assisted access
LDPC	Low-density parity-check
LTE	Long-term evolution
M2M	Machine to machine
MAC	Medium access control
MANO	Management and orchestration
MEC	Multi-access edge cloud
MIMO	Multiple input, multiple output
MiTM	Man-in-the middle
ML	Machine learning
mMTC	Massive machine-type communication
mmWave	Millimeter wave
MR	Merged reality
MVNO	Mobile virtual network operators

Term	Definition
NaaS	Network as a service
NF	Network function
NFV	Network function virtualization
NGMN	Next generation mobile networks
NGC	Next generation core
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NOMA	Non-orthogonal multiple accesses
NR	New radio
NS	Network slicing
NSA	Non-standalone
OEC	Open edge computing
OFDM	Orthogonal frequency-division multiplexing
OMEC	Open mobile edge cloud
ONF	Open Networking Foundation
OPEX	Operational expenditure
ONOS	Open Network Operating System
OPNFV	Open platform network virtualization
OSS	Operational support system
OTT	Over the top
OVS	Open vSwitch
PGW	Packet gateway
PHY	Physical layer
PoC	Proof of concept
QoS	Quality of service
RAN	Radio access network
RE	Range extension
RRSA	Rapid reaction standardization activity
RSRP	Reference signal received power
SDN	Software defined network
SDO	Standards developing organization or standards development organization
SIEMs	Security information and event management
SIM	Subscriber identification module
SLA	Service level agreements

Term	Definition
SON	Self-optimizing network
TDD	Time-division duplex
TDMA	Time division multiple access
TPM	Trusted Platform Module
TSDSI	Telecommunications Standards Development Society India
TTI	Transmission time interval
UAV	Autonomous aerial vehicles
UE	User equipment
UL	Uplink
UP	User plane
URLLC	Ultra-reliability low latency connection
V2I	Vehicle to infrastructure
V2V	Vehicle to vehicle
V2X	Vehicle to everything
vEPC	Virtual evolved packet core
VNF	Virtual network function
WRC	World Radiocommunication Conferences
WG	Working group

ANTI-TRUST 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-SA. That policy can be found at https://standards.ieee.org/develop/policies/antitrust.pdf.



FutureNetworks.ieee.org/roadmap

IEEE INTERNATIONAL NETWORK GENERATIONS ROADMAP, 1ST EDITION