Market Dynamics and Security Considerations of 5G

Anand R. Prasad[1], Sivakamy Lakshminarayanan[2] and Sivabalan Arumugam[2]

[1]*NEC Corporation, Japan*
[2]*NEC Technologies India Private Ltd, India*
E-mail: anand@bq.jp.nec.com; sivakamy.l@india.nec.com; sivabalan.arumugam@india.nec.com

Received 22 March 2018;
Accepted 18 April 2018

Abstract

The 5$^{\text{th}}$ Generation (5G) of mobile communication systems will bring massive changes in the dynamics of the Information and Communication Technology (ICT) industry. The applications of 5G technology are well-positioned to address the ever-increasing demand for enhanced service experience. With digitization on its way to touch every part of life, Internet of Things (IoT) will be integral part of 5G from the very beginning; this is unlike 4G where IoT came later. However, open issues such as market demand, technical viability, economic feasibility of adopting 5G and related business dynamics do exist. This paper discusses such issues and more importantly, the security considerations in the world where everything will be connected.

Keywords: 5G, IoT, 5G Security, NFV, IIoT.

1 Introduction

The advent of the fifth generation of mobile communication (5G) is expected to be a one-stop solution for almost all requisites of a hyper-connected, intelligent and mobile society. It is all set to bring about a massive paradigm shift in

Journal of ICT, Vol. 5_3, 225–250. *River Publishers*
doi: 10.13052/jicts2245-800X.532

business models and contribute extensively to socio-economic growth in terms of productivity, energy, cost efficiency and sustainability.

5G manifests itself as an inclusive, modular, agile, flexible and scalable end-to-end system. The use-cases of 5G can be classified into eight families [1] based on specific service requirements. They are broadband access in dense areas, broadband access everywhere, higher user mobility, massive Internet of Things (IoT), extreme real-time communications (RTC), lifeline communications, ultra-reliable communications and broadcast-like services. Broadband access in 5G will be so much more than what legacy telecom networks have offered. 5G will make ubiquitous connectivity possible even in dense areas where the average number of devices is in the order of few thousands per square kilometre. It will also be an all-pervasive network that guarantees consistent user experience anywhere, urban or rural, indoors and outdoors. 5G will also cater to the ever-increasing demand for on-the-go mobile services, even for highly mobile vehicles. This will also include in-vehicle services ranging from navigation and entertainment to more sophisticated services like autonomous driving and vehicle diagnostics. Massive IoT augments a myriad of devices to support applications such as smart cities, smart agriculture, smart wearable etc. Extreme RTC includes services such as tactile internet that require ultra-low latency real-time communication. Lifeline communication includes agile, dependable public safety and emergency services. Ultra-reliable communications cover life-critical use cases such as remote surgery, automated traffic control, and industrial automation which require ultra-low round-trip latency with ultra-high reliability. Unlike legacy broadcast, one can expect personalized and customized real-time content broadcast targeted at specific user groups in 5G.

This calls for an enhanced, dynamic, heterogeneous environment which is capable of handling a plethora of service requirements. To cater to the versatility of requirements for the use-cases, 5G harnesses the power of virtualization of network functions to provide various services simultaneously using the same underlying infrastructure. 5G, by design, has the flexibility to harbour a myriad of services on a single platform. It essentially works by "slicing the network" to fire up multiple parallel instances of the same network function (i.e. the network resource) on demand [1]. This way, a hard limit is set on network resource utilization by a specific type of service or use-case allowing different set of security services and Quality of Service (QoS) to be applied based on pre-defined or dynamic policies.

The organization of the paper is as follows: In Section 2, we discuss the market dynamics of future mobile communication networks. In Section 3,

we look at the functional aspects of 5G. We elicit the crucial security related considerations for 5G in Section 4. Security as a business enabler is discussed in Section 5. Conclusion and thoughts on future work are given in Section 6.

2 5G Market Dynamics and Security

The telecom industry today has the potential to bring about a paradigm shift in business methodology and revolutionary transformation in the market. The stakeholders are poised to make use of the new opportunities and business avenues stemming out of technical feasibility, economic viability and more importantly, scalability. The key factor driving this revolution is the move towards digitalization to connect everything [2]. Figure 1 illustrates the various factors impacting the market of future mobile communication networks.

With operators embracing Software Defined Network (SDN) [3] and Network Function Virtualization (NFV) [4] as an integral part of the 5G mobile network, a variety of services can be run simultaneously on virtual machine (VM) instances using the same underlying infrastructure. With NFV and cloud, "softwarized" instances of the network entities could be brought up

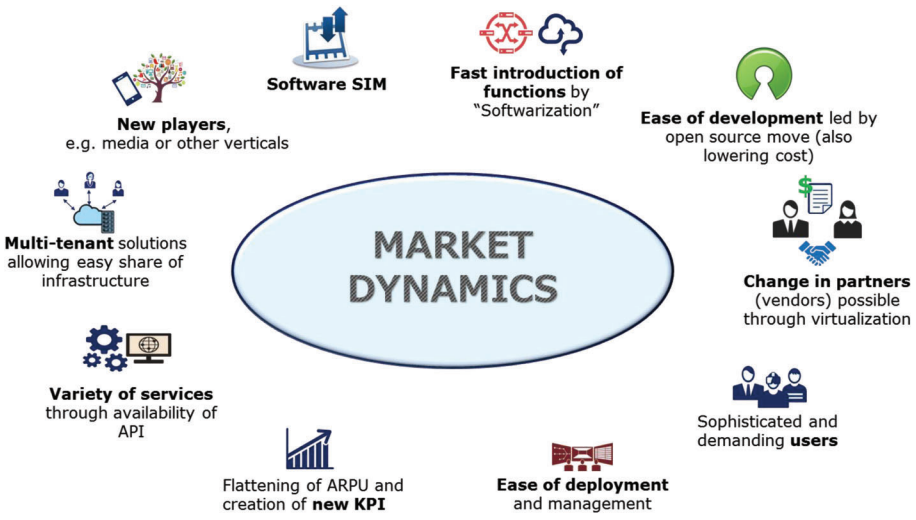

Figure 1 Market dynamics of future mobile communication networks.

on-demand. This allows multi-tenancy [5] in which multiple users access the same resource (instance of the resource running on the cloud) simultaneously without compromising service (including Quality of Service (QoS)) and security requirements. NFV Management and Organisation (MANO) framework facilitates ease of deployment by allowing flexible on-boarding of virtual network function (VNF) packages and new network services (NS). The VNF manager, a functional block of MANO, coordinates configuration and manages the lifecycle of VNF instances [6].

Digitalization offers the gateway to reimagine and reinvent the business verticals. Entrance of new players offering platform-based solutions will disrupt the industry value-chain. Solutions targeting specific industry verticals such as media, manufacturing, automotive, healthcare, financial services and public safety will bring about agility in terms of flexible business models with interchangeable market players and new partnership models between the stakeholders. The industry will also see widespread use of open source hardware and software for rapid, cost-effective and agile development of products and services [2].

Recent evolution of the Subscriber Identity Module (SIM) has focussed on embedded solutions and remote provisioning, both relying on a physically secure hardware element, for credential provisioning in Machine-to-Machine (M2M) [7] and IoT usecases. However, complete "softwarization" of the SIM wherein there would be no hardware layer has also been under speculation. With such virtual SIMs, there will be no need for large-scale distribution of SIM cards, especially for M2M/IoT devices. It will also prevent the cumbersome process of replacing faulty SIM cards [8]. The manufacturing and logistical benefits of soft SIMs could attract significant research space and market share in the coming years [9]. However, realization and usage of soft SIMs require stringent security considerations.

With everything getting connected, there will be an increased need for data and information security. 5G holds security business potential across areas like healthcare, retail, banking and finances, agriculture, automotive and even, home appliances. The trump card of businesses will be security. Baseline security aspects (Confidentiality, Integrity and Availability) will apply across all domains in the network. Moreover, it can be envisaged that different security considerations will be applicable for different services. Pay-per-use security add-ons can also be made available to the users (customized security services). Security as a business enabler is discussed in Section 5.

3 What 5G has In-Store?

In this section we look at various aspects, from network to users, which are changing as we move towards 5G.

3.1 (Core) Network

The 5G core network is expected to handle exponentially more users, connecting via heterogeneous access technologies, than legacy telecom networks. 5G network management is faced by challenges ranging from limited resource availability to varying, at times conflicting, management, security and QoS objectives of the manifold use-cases. It is vital that the 5G network is capable of regulating and optimizing resource allocation and utilization.

As we move ahead, virtualization technology (NFV and SDN) for mobile core networks will play a vital role in cost reduction while achieving the desired quality requirement. This will lead to the network (core network) being increasingly built of off-the-shelf hardware and open source software. This will pave the way for mobile networks to become increasingly cloud based.

NFV will facilitate networks to be launched on-demand for a specific service using the concept of Network Slicing. A network slice is a logical instance of network function(s) that can be created, deployed, utilized and removed on-demand based on service requirements [1]. This way, the virtualized vertical instances of the network running on the cloud fulfil specific requirements in contrast to horizontal networks today that cater for all services.

The use of virtualization and cloud also offers more flexibility and accessibility to the network. This will also lead to the core network border being extremely flexible. The core network could be one software module or multiple modules located in different parts (physically) of the network be it at server farm or in a box close to the base-station – Mobile Edge Computing (MEC) [10].

3.2 Radio Access Technology (RAT)

Radio access technology will see several improvements with data-rates varying from few bits going up to several gigabits and latency going down to micro- if not nano-seconds.

The power of MEC [10] can be harnessed to enable rapid and flexible deployment. Radio access network (RAN) will also become partially virtualized and cloud based. The properties of cognitive radio [11] can be

integrated with the RAT functionality to enforce slice-specific or use-case specific security policies. By infusing adaptive learning on the cognitive radio platform, we can create an intelligent, flexible, energy efficient and scalable radio access network.

Relying on macro cell towers will no longer be sufficient to address the demand, especially in regions with high-density of devices. 5G coverage will involve use of small cells, femto-cells [12] and interactions between the macro and micro cell towers with private hotspots to augment network capacity and connectivity. Such a heterogeneous topology with "relays" will be vital in providing network connectivity to remote, inaccessible regions, especially during disasters. Device-to-Device (D2D) [13] discovery and communication will enable mobile devices to be used as relay nodes to create the meshed network. This provides a relayed pathway for remote devices to get connectivity during emergency situations. Solutions similar to Isolated E-UTRAN Operation for Public Safety (IOPS) [14, 15] could be used to maintain the connectivity between the devices, offering mission-critical services even when backhaul connectivity may not be fully functional.

Another possible solution for providing 5G radio coverage in remote areas is the use of a mesh of Unmanned Ariel Vehicles (UAVs) acting as Remote Radio Heads (RRHs), which are then connected to the virtualized instance of the RAN running on the cloud. This solution can be used by paramilitary forces for swift and ad-hoc deployment of a temporary semi-mobile (restricting mobility over the target region) network. Combined with wireless short-range communication protocols such as Bluetooth, ZigBee and Near-field Communication (NFC), this could also be used for defence applications [16]. Figure 2 illustrates the combined use of RRHs mounted on UAVs and D2D communication for providing network connectivity in the event of disasters.

It is also possible that slice-based instances of the cloud-part of the RAN may also be used. The slices can be based on the type of access, type of service, service requirements (data-rates, volume of data, latency) and security requirements. Different priority levels may also be set on the QoS for each RAN slice depending on the requirements. With rapidly evolving techniques for softwarization of entities in the radio communication system, mass deployment of Software-defined Radio (SDR) [17] is also expected.

3.3 Spectrum

The spectrum used for 5G will be different from previous technologies. The spectrum will have implications on coverage and behaviour of radio

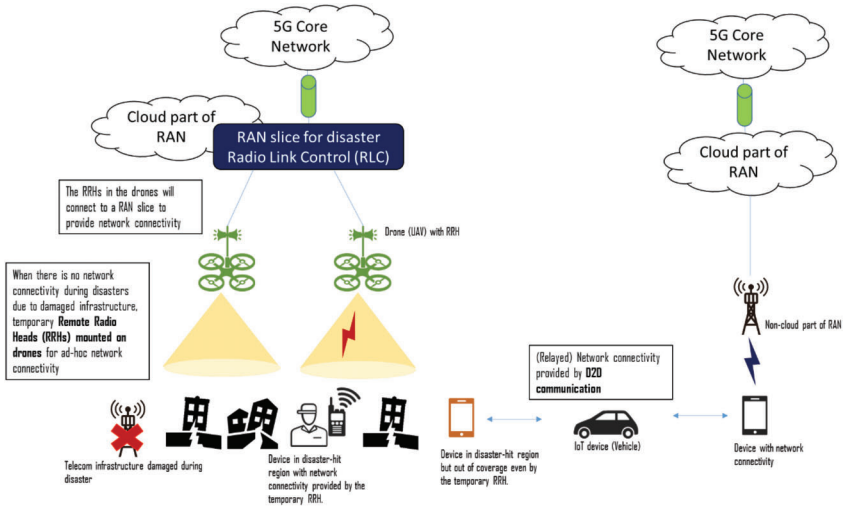

Figure 2 Disaster communication using temporary RRHs mounted on UAVs and D2D communication.

access technology. There have been discussions of both higher GHz bands and sub-6 GHz bands. The millimeter wave (mmWave) spectrum has been successfully tested for point-to-point infrastructure links having total line-of-sight (LOS). But, it does have its share of disadvantages – attenuation and inefficiency in non-line-of-sight (NLOS) environments [18]. Other fronthaul technologies such as free space optical (FSO) for 5G Ultra dense cloud small cell network (UDCSNet) have also been discussed [19]. But, the performance of a FSO link can be degraded sharply in the presence of thick clouds, severe fog, or dust storms. To achieve both high capacity and carrier availability, a hybrid FSO/mmWave approach has been proposed [20]. For low range coverage in both LOS and NLOS environments, sub 6 GHz licensed spectrum would be a favourable option due to its higher spectral efficiency and higher tolerance [21].

With the arrival of 5G, we should also expect aggregation of cognitive radio in mobile networks with unlicensed band as well as usage of unlicensed band technologies. The convergent usage of licensed and unlicensed spectrum opens up new research and business opportunities. We can also expect wide-scale deployment of Sensing-based Spectrum sharing (including TV white spaces) [22] to allow multiple users transmit over the same bands with minimal interference.

3.4 Security Credentials

Given the variety of scenarios and technologies expected to be offered by 5G, it is worth questioning whether the security credentials should stay the same as today or whether there will be change in technology for storage of credentials. Change in security credentials could have implications on authentication and other security mechanisms.

On the network side, storage is in terms of whether the security credentials are stored at the mobile network domain or at partner domain. The location in which credentials are stored and processed will have implications on the authentication end-point and transfer of session related security credentials to appropriate network functions after completion of authentication.

With regard to security credential storage in devices, one can consider three different forms of storage (1) secure hardware environment as we have today in the form of Universal Integrated-Circuit Card (UICC) that is commonly known as SIM card, (2) embedded secure hardware environment, e.g. a UICC or similar device is implemented in a modem, this brings us to something like embedded SIM and (3) some form of software.

The IoT, one of the main verticals of 5G networks, makes it possible for a huge number of "intelligent" devices to communicate with each other seamlessly. This calls for a secure hardware environment in the user device which is capable of remotely managing multiple subscription profiles and credentials. It is also possible for the Mobile Network Operator (MNO) to enable and disable profiles on the eUICC and make a switch between two profiles over-the-air (OTA) [23, 24]. This contributes to enhanced flexibility for SIM manufacturers to locally provision a globally manufactured product to suit customer needs by offering secure SIM personalization and customization options.

There may also be complete softwarization of the SIM (soft SIMs), as mentioned in Section 2, offering more flexibility and dynamicity to credential storage and processing.

3.5 End Devices

End devices will see huge transformation backed by technology enhancements that we are witnessing around us. Already with the arrival of 4G, there have been an upsurge in the demand and usage of smartphones and over the top (OTT) services. The shift towards 5G will see increased number of smart "devices" as well as a whole variety of IoT devices associated to a plethora of services. Wearables will be household necessities while virtual or augmented

reality (VR or AR) type devices will be commonly available. This will also lead to the business stakeholders embracing off-the-shelf, open source devices available in the market since a while to strike a balance between demand and supply.

With 5G, we should expect all types mobile devices (like smart devices, IoT, VR, AR, Vehicles) to be directly connected to the Internet, making them reachable over Internet Protocol (IP) addresses. As the number of devices swells exponentially, there will be a definitive adoption and widespread usage of IPv6 [25]. Considering the IoT use-cases, there will be devices requiring long battery life (say 10 years) that are expected to work at very low data rates.

3.6 Services

Apart from voice and broadband, services tailor-made for VR, AR, IoT, smart devices, vehicles and many more will spring up as 5G will provision a unified platform that can cater to a variety of requirements.

These services may be provisioned by the mobile operator or by a third party service providers. This can be done with and without any direct business relation between the service providers and the mobile operators.

With virtualization and network slicing, localized services (services available in a specific region or to a specific group of users) will become more and more significant. The scenario where a user walks into a library and informative graphics in the AR gear show the location of books based on their preference, as illustrated in Figure 3, is a typical example of localized services. Location-specific services such as, parking lot pre-booking, an interactive map of a mall, a dashboard showing discounts and offers running in various shops as the user walks by could be made available to shoppers upon entering the mall premises. The availability of such services could become a source of revenue. It will also be invaluable for tourists and first-time visitors. Another example of using AR for providing information on-the-go for travellers is shown in Figure 4. AR gears, equipped with facial recognition modules, could help the law enforcement agents to identify individuals even in a huge crowd. With Artificial Intelligence (AI), surveillance cameras (IoT devices) can monitor individuals engaging in suspicious activities and alert the officials almost instantaneously. On a larger scale, such services could also be customized for defence applications. Slices may also be localized networks in themselves; there will be an increased demand for (Virtual) Network-as-a-Service (NaaS) providers for IoT and M2M.

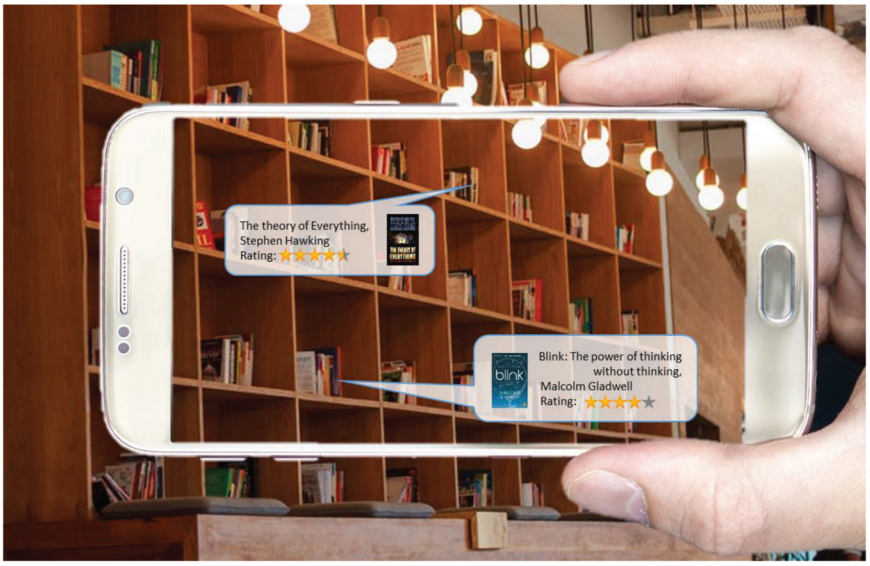

Figure 3 AR application showing location and details of books in a library.

To support integration of services for a specific use case, the applications need to be able to communicate with each other for data sharing. This involves mutual interaction between the software applications and also between the application and underlying infrastructure.

3.7 Business

There is already a rampant change in the business model of mobile operators. One such change is in the form of Application Programming Interfaces (APIs) [26] being made available for third parties to launch different kinds of services over the mobile network.

With 5G in picture, we will also see operators getting in partnership with other companies to provision the content (linear and interactive) and services. This would mean that the partners essentially own the subscriptions while the operator would be responsible for the mobile telecom infrastructure and correct usage of the licensed spectrum.

With the trend of multi-device ownership (a person owning and using multiple devices) and multi-device multi-user trends (several people sharing multiple devices especially in home automation and V2X), we can expect flattening of Average Revenue Per User (ARPU) [2]. The harmonization of

Figure 4 Localized service providing useful information for travellers.

ARPU will lead to business models framing new Key Performance Indicators (KPIs) for business intelligence. Providing services with good Quality of Experience (QoE) will be inevitable for customer retention and business contingency.

With digitalization driven by Industrial IoT (IIoT) [27], more emphasis will be on Business-to-Business (B2B). This will eventually transform the existing operation-driven business paradigm to information-driven and service-oriented paradigms. We can expect synergy between content providers, service providers and network operators (Mobile Network Operators (MNOs) and Mobile Virtual Network Operators (MVNOs)) which can lead to new business models and service level agreements. Scenarios in which more than two stakeholders are involved are also possible. Multi-party contract models, which rely on smart, digital contracts could also come into being. The use of smart contracts for dynamic service level agreements is a topic in itself and is not discussed in depth in the paper.

3.8 User Space

5G will have much deeper penetration in the society than any of the technologies to-date. This equates to technology being used by tech-savvy individuals and also Information and Communication Technology (ICT) first-timers who will leap-frog directly to the new technology. The former would need more personalized and configurable service options to choose from while the newbies would require a more user-friendly, interactive interface for smoother transitions. Customized services will have to be made available for the different classes of users.

5G will play a major role in enhancing the quality of life involving not just human beings but also animals (e.g. for vital information), plants (e.g. for watering) and "everything" (Internet of Everything (IoE) [28]), which will be inter-connected with each other and the internet. It is prudent to adopt economically viable solutions so as to make the technology reachable to people from all walks of life.

4 Security Considerations for 5G

In this section, we discuss the security considerations for 5G. Security vulnerabilities, attacks and solutions are separate topics in themselves and are not discussed in this paper.

4.1 (Core) Network

As discussed in Section 2.1, the core network will cater for connections via multiple access technologies and provide services of several types by making use of SDN, NFV and cloud. Several security aspects need to be considered while designing and utilizing a virtualized platform, probably hosted on the cloud.

4.1.1 Virtualization

A mobile network has to store and handle several security credentials of its subscribers, active or recently active. The network must also store security parameters and credentials used for securing the connection between network functions. This becomes even more difficult when the network functions are virtualized as the security credentials in the cloud will potentially be accessible to attackers. Also, attack from one Virtual Machine (VM) could flow to other VM instances or tenants [29]. The attacked VM may act as a bot, thereby endangering the whole network.

Based on the discussion it is clear that secure boot and secure storage of security credentials is a security base-line for virtualization. The security credentials may have to be managed across all virtualized instances of the network functions. In such a case, isolation between the VMs is of paramount importance. Need for isolation becomes more profound during inter-operator communication in a multi-vendor ecosystem.

With NFV, multiple consumers are served by the same logical instance (of physical resources) running on the cloud simultaneously using the concept of multi-tenancy [5]. Such resource-sharing models pose serious threats such as data leakage, cross-network eavesdropping, and even Man in the Middle (MitM) attacks. Moreover, misuse of the shared resource by one tenant could lead to single point of failure for all harboured tenants. Logical security isolation among the tenants is necessary to ensure that one tenant cannot interfere/tap/modify communication between the resource and another tenant. Beach-heading of attacks by a compromised tenant should be prevented. Strong access control mechanisms should be implemented to prevent unauthorized elevation of privilege. Another aspect here is congestion control (endangering availability of resources) – any tenant's/group of tenants' resource consumption should not affect the QoS of another tenant.

The mobile network security perimeter will under-go a major change to accommodate virtualization of modular network functions. So, existing defence mechanisms will not hold good in deterring attacks at network borders. The network border will be pushed deeper in the network thereby exposing its vulnerabilities further; attackers will be able to reach much deeper into the network than ever before.

It goes without saying that baseline security considerations including hardening, Transmission Control Protocol (TCP)/ Internet Protocol (IP) stack [30] security, Operating System (OS) [31] security, hypervisor [32] security, password management will become indispensable. Security orchestration, besides secure orchestration, and security monitoring will be required. Other virtualization related security aspects covered elsewhere [33, 34, 35] are not discussed in this paper.

4.1.2 Cloud

Cloud is much more than virtualization; virtualization is an enabler of cloud. VMs deployed in the cloud can migrate from one location to other. Considering VM instances that can be created and migrated on-demand, the security and networking related credentials and configuration parameters are

constantly at risk of exploitation; the network functions (and therefore the network itself) become vulnerable.

All credentials or configuration parameters associated with a migrating instance of a network function must be removed from the source location before migration. Similarly credentials and configuration parameters must be secured during the migration (information in transit) as well. The benefits of this are two-fold: (1) storage of old credentials and configurations could lead to unnecessary misconfigurations in the network (2) the network functions could become targets of attack. It is also a good practice to ensure that the security credentials are refreshed or re-derived at the target location. This is to ensure that the target location is secure even if the source may have been compromised.

4.1.3 Slicing

As mentioned in Section 2.1, network slicing will be brought about with the help of virtualization and cloud, although one could argue that slicing is doable without these technologies as well. As slicing is meant to provision an instance of the network for specific service, it is also possible that various radio technologies will be connected to a given slice. This leads to several security considerations. Firstly, with a world of services being hosted on the cloud, mechanisms to identify and track subscriptions, slices and instances of network functions are required. With 3rd party slices on offer, there may be a need for separate authentication methods between the user and the external vendor (facilitated by the network operator). It is also vital to ensure that a user is authorized to access the service requested by them. Authorization may have to be done per slice (depending on the user's subscription) as charging may be done on a pay-per-use basis.

The concept of network slices also redefines how the control plane (control signals to and from the network) and user plane (data) look like. Basic security aspects such as confidentiality, integrity and replay-protection will have to be considered at the security end-points. The kind of security mechanism used will be impacted by virtualization; it needs to be ensured that the network traffic for one slice is isolated from that of the other. This is crucial for privacy and to prevent fraudulent charging as well. Care should be taken that confidential information of users are not leaked to 3rd party service providers (to ensure user privacy).

There are also cases in which inter-slice communication may be required. Security aspects for such scenarios involving communication between virtualized instances of network functions must be considered. Further, security

mechanisms during mobility for all cases (within slice, between slices and between radio access technologies) and for all states (a device and/or service might be in) must ensure forward and backward security.

With all these, the system should also support backward compatibility with existing mobile networks. In this case, the security credentials and configuration parameters used in 5G should never be revealed to the legacy networks.

4.2 Radio Access Technology (RAT)

Radio access technology will see several improvements with data-rates available from few bits going up to several gigabits and delays going down to micro- if not nano–seconds. As discussed in Section 3.2, Radio access network will also become partially virtualized and cloud based. Let us now look at security considerations:

4.2.1 Virtualization and Cloud

With virtualization, the radio access network (or at least virtualized part of the radio access network) will face security issues similar to the core network, as mentioned in Section 4.1.1. Additional implications due to RAT and RAN characteristics will appear. Security provisioning mechanisms may be different for the type of RAN. This will have impacts on the type of algorithms and protocols used.

The combined need for increased and uninterrupted radio coverage, higher throughput, much higher density of devices with varied levels of acceptable latencies necessitate the move towards a partially cloud-based radio access network. Additional security consideration will be required for introduction of new interfaces to the core network and within the radio access network including interface between the cloud part and non-cloud part. With RAN slicing, multiple virtual interfaces should be integrity, confidentiality and replay protected. Also, secure identity management techniques will also be required on the RAN cloud apart from secure storage and processing of credentials.

4.2.2 Data-rates and Delays

For IoT and M2M devices requiring very low data-rates, going down to few bits per day, we will have to consider the extent of security (be it authentication, confidentiality, integrity or otherwise) that can be provisioned. Such devices will also be resource-constrained in terms of battery life, computation and

memory. This calls for light-weight authentication methods that should not run for every communication. Even when run, they should be performed with minimum round-trip. Light-weight and fast re-authentication techniques could be employed to periodically authenticate devices and refresh the security credentials, if required. To reduce computational latency, one solution will be to reduce security related bits of keys (e.g. integrity and confidentiality) and parameters sent OTA. Security and cryptographic algorithms must be energy efficient and optimized to work for resource-constrained devices.

On the other hand, there are high data-rate devices with higher battery and computational resources; examples include the smartphones or tablets, IoT devices like vehicles, IIoT devices like machineries in factories and virtual or augmented reality (VR or AR) devices used for gaming or real-time services. The processing complexity of security functions and algorithms should be at a bare minimum for devices that require high data rates. At the same time, higher data rates are provisioned by decreasing the overhead bits in radio interface that in turn has implications on bits that can be budgeted for security.

IIoT and healthcare services require very low latency, high throughput and more reliability. In such a case, the powerful but light-weight security mechanisms need to be used. The data and signalling channel must be protected against MitM attacks to prevent data tampering, which can lead to fatal consequences. Strong integrity protection must be enforced to ensure that the data has not been modified. Confidentiality protection can be applied for cases with more relaxed latency requirements.

For D2D communication, security aspects such as authentication, authorization, access control for devices that are not directly connected to the core network need to be studied. There is also a greater chance of eavesdropping and MitM attacks in such a scenario.

Adoption of SDR is accompanied with increased vulnerability to security attacks. Softwarization of RAT elements puts sensitive information such as security credentials and configuration data at risk. Threats related to Operating systems are also applicable [31]. Without proper security mechanisms in place, unauthorized use of SDR resources may also occur. Threats associated with cognitive radio are discussed in [36].

Security considerations mentioned under slicing (authentication, key management etc.) part of previous section on (core) network are also valid for radio access network and radio access technology. Enhancements like beamforming [37] and their security implications should also be considered.

4.3 Spectrum

Aggregation of licensed with unlicensed band for which solutions are already available today, requires consideration of resource availability, authentication, integrity, confidentiality, replay protection and authorization. Use of cognitive radio will mean that different devices with different priorities will exist. This will require good means of authorization to access the radio resource. Threats related to spectrum sharing such as Primary User Emulation (PUE) attacks, Spectrum-Sensing Data Falsification (SSDF) attacks, Spectrum Utilization-based Location Inferring (SULI) attacks and Beacon Falsification (BF) attack are discussed in [38]. It is also worthy to note that security policy inference carried out by a policy-based cognitive radio needs to be executed within a very tight time window.

4.4 Security Credentials

With 5G, there could be change in security credentials and how they are stored. Each of the three different forms of storage mentioned in Section 3.4 have different implications on business model and security. Soft SIMs will rid the dependency of network operators on any 3rd party for storage medium (such as UICC). However, storage of security credentials in software has severe security implications as they can be easily compromised. One can also expect that provisioning of security credentials OTA will replace or at least supplement hard-coded or pre-programmed credentials. OTA mechanisms will require a secure channel to be established between the parties involved in it to prevent credential leakage. Mechanisms to reset the device to factory default credentials might be needed; basically several aspects of credential management will be expected, potentially, beyond what we have seen today.

In spite of the security loopholes, software could still be considered as an option for businesses with very cost of devices and services. In such cases, the trade-off between security and cost at the device level can be balanced by implementing faster means of attack identification and automated control mechanisms at the server. This brings us to powerful Intrusion Detection Systems (IDS) with adaptive learning capabilities (using ML and AI) to be deployed in the application servers.

4.5 End Devices

With an all-IP network, reachability directly from Internet will mean that devices will be more prone to cyber-attacks as we see today in personal computers arena or the Information Technology (IT) world.

Long-standing devices (such as sensors) that are expected to work at very low data rates will face other security issues. It is possible that the cryptographic algorithm implemented such devices will be cracked during the lifetime of the device. There may even be cases in which the device may end up being used for purposes other than what it was originally designed for. Both of these scenarios can lead to successful attacks on the device. For such cheap, mass-produced devices, it is likely that all algorithms will be hard encoded. So, technically and economically, change the algorithms or device functionality to counter the attacks will not be feasible.

As devices by themselves will not be capable of provisioning adequate security, network-assistance will have to come in picture. The network can support the devices in terms of security by monitoring the traffic, analysing the traffic for potential security issues and detecting anomalies. This can be done by deploying IDSs equipped with ML capabilities to classify traffic and identify security issues in real-time. In case of security issues, the network should be capable of taking necessary actions as per the policy of user or operator. Thus, from the very beginning, the network could be designed to cater for security requirement of specific types of devices or services.

Open source devices could cause several issues, especially if all protocol layers and all parts of the device are accessible to the user. An attacker with such device could, for example, misuse the control plane protocol stack that will lead to a variety of attacks on the mobile network. *Lipp et al.* [39] demonstrated that certain hardware vulnerabilities could be exploited to steal passwords and sensitive information. It is necessary that appropriate security protocol stacks are employed at all applicable layers.

As the use of APIs increases, advanced code injection and execution attacks may be possible. This can cause misconfigurations in the device and render them useless. According to The Open Web Application Security Project, applications may unintentionally share session tokens with malicious actors, allowing them to impersonate legitimate users.

4.6 Services

With emergence of the technology that supports a huge variety of services, different ranges of devices and source(s) of services can expected. Provisioning of any type of service will require authentication or proper authorization. Misuse should be expected otherwise.

Over the top (OTT) services have the potential of leading to potential cyber-attacks through malware, phishing etc [40]. It is also worthy to note

that Data analytics will play a major role in service optimization. It will play an integral role in service customization and user-based personalization. Apart from this, misuse of sponsored data, a source of revenue for mobile operators, could endanger user privacy and could lead to operators suffering financial loss.

Public safety security work has been done extensively in 3GPP for cases like D2D communication as well as situations where the radio network is not connected to the core network. Such security solutions will also be required in 5G from the very beginning. The solutions might go well beyond public safety and create a profitable niche market.

5 Security as a Business Enabler

We are already seeing a reformation in business model of mobile operators. One such change is in the form of APIs being made available for third parties to launch services over the mobile network. This not only requires SLAs between the MNO and the 3rd party service provider, but also requires enhanced security. This is because the network resources essential for mobile network functioning are exposed to an external entity (in the 3rd party domain), making them susceptible to attacks. Attacks are now possible deeper in the network than ever before [41].

The world of intelligently and securely connected devices and services open up new business opportunities with minimal impact to the infrastructure thereby minimizing cost and integration overheads. With multi-party contracts and dynamic partnerships, a whole set of security requirements also associated to the partner will have to be fulfilled including authentication and key management while safe-guarding and inoculating the internal network.

The user space will also see major changes. Tech-savvy, perspicacious users who understand the implications of security and privacy will prefer varied levels of configurable security settings, some of which can be monetized. Novice users will have to wade through common security attacks such as phishing and social engineering. Creating awareness across all levels of users becomes necessary. It is also possible for the security configurations to be visible to the user, probably communicated to the device via APIs. The user could also be made aware of the security options available for a specific service so that they can choose whether this is secure enough for the service used [41]. An example use-case is the user being prompted on the option of encryption of voice calls, which the user may choose to activate (for a fee) in case sensitive information needs to be communicated during the call.

5G will have to cater for all types of users at adequate price level so that security becomes reachable to all. Therefore, it is necessary to consider Life-cycle security considerations for products and network as a whole. Security life-cycle management should be integrated into the product/service development life-cycle. Solutions enabling real-time monitoring of telecom networks that do not compromise privacy will be required.

6 Conclusion

5G provides enhanced, dynamic, heterogeneous environment; an umbrella for a plethora of services realized by seamlessly incorporating SDN/NFV technologies. For 5G to function properly, we will need baseline security standardization for aspects such as authentication, confidentiality and integrity of messages etc. Besides standardized security mechanisms, security monitoring, analysis, control with real-time data analytics and artificial intelligence, are compelling business requirements.

It will be essential to take care of baseline security, i.e. security for OS, TCP/IP stack, password management, logging etc. Security assurance, i.e. testing of network functions and live network, also forms a part of baseline security. One could consider embedding of security assured certification in the network functions or protocols to automate the proof of level of expected security. At the same time, it will be essential that 5G solutions provision means for rapid changes in-case of vulnerability or attack identification, i.e. waiting for patch cycle becomes unnecessary.

New technology development will be required as mentioned throughout the paper. This includes cryptographic algorithms, security credentials and storage. Security monitoring and real-time analysis will also become an important commercial thrust point in business. Particularly we will need improved analysis technologies embracing machine learning and AI that will have negligible false positives without human intervention.

Even after everything, it will be essential that the network also provisions security as a service. This security provisioning by the network will become a new form of profitability for the value-chain as it will truly make security a business driver of mobile networks – secure network as a service – embracing the fact that one size does not fit all!

References

[1] Alliance, N. G. M. N. 5G white paper. "*Next generation mobile networks, white paper*" (2015).

[2] NEC, "Making 5G a Reality." http://www.nec.com, 22-Feb-2018. [Online]. Available: http://www.nec.com/en/global/solutions/nsp/5g_vision/doc/wp2018ar.pdf. [Accessed: 12-Mar-2018].

[3] Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., and Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials, 16(3), 1617–1634.

[4] Li, Yong, and Min Chen. "Software-defined network function virtualization: A survey." *IEEE Access* 3 (2015): 2542–2553.

[5] Koponen, Teemu, Keith Amidon, Peter Balland, Martín Casado, Anupam Chanda, Bryan Fulton, Igor Ganichev et al. (2014). "Network Virtualization in Multi-tenant Datacenters." In *NSDI*, vol. 14, pp. 203–216.

[6] ETSI, "Network Functions Virtualisation (NFV); Management and Orchestration", ETSI GS NFV-MAN 001 v.1.1.1, 2014.

[7] 3GPP, "Service requirements for machine-type communications," 3GPP TS 22.368 V13.0.0, 2014.

[8] GSMA Intelligence, "The future of the SIM: Potential market and technology implications for the mobile ecosystem", (2017)

[9] GSMA Intelligence, "Understanding SIM evolution", (2015)

[10] European Telecommunications Standards Institute, "Mobile Edge Computing – A key technology towards 5G", ETSI White Paper No. 11, (2015)

[11] Hong, Xuemin, Jing Wang, Cheng-Xiang Wang, and Jianghong Shi (2014). "Cognitive radio in 5G: a perspective on energy-spectral efficiency trade-off." *IEEE Communications Magazine* 52(7), 46–53.

[12] Galinina, Olga, Alexander Pyattaev, Sergey Andreev, Mischa Dohler, and Yevgeni Koucheryavy (2015). "5G multi-RAT LTE-WiFi ultra-dense small cells: Performance dynamics, architecture, and trends." *IEEE Journal on Selected Areas in Communications*, *33*(6) 1224–1240.

[13] Asadi, Arash, Qing Wang, and Vincenzo Mancuso. "A survey on device-to-device communication in cellular networks." *IEEE Communications Surveys & Tutorials* 16.4 (2014): 1801–1819.

[14] 3GPP, "Study on isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety," 3GPP TS 22.897 v13.0.0, 2014

[15] 3GPP, "Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Stage 1," 3GPP TS 22.346 v14.0.0, 2017

[16] Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., and Ladid, L. (2016). Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications, 34*(3), 510–27.

[17] Sun, S., Kadoch, M., Gong, L., and Rong, B. (2015). Integrating network function virtualization with SDR and SDN for 4G/5G networks. *IEEE Network, 29*(3), 54–59.

[18] Niu, Y., Li, Y., Jin, D., Su, L., and Vasilakos, A. V. (2015). A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges. *Wireless Networks, 21*(8), 2657–2676.

[19] Zhang, Haijun, Yanjie Dong, Julian Cheng, Md Jahangir Hossain, and Victor CM Leung. "Fronthauling for 5G LTE-U ultra dense cloud small cell networks." *IEEE Wireless Communications*, *23*(6), (2016): 48–53.

[20] McKenna, Timothy P., Juan C. Juarez, Jeffrey A. Nanzer, and Thomas R. Clark (2013). "Hybrid millimeter-wave/free-space optical system for high data rate communications." In *Photonics Conference (IPC), 2013 IEEE*, pp. 203–204. IEEE

[21] Wei, Lili, Rose Qingyang Hu, Yi Qian, and Geng Wu (2014). "Key elements to enable millimeter wave communications for 5G wireless systems." *IEEE Wireless Communications, 21*(6), 136–143.

[22] Akhtar, Auon Muhammad, Xianbin Wang, and Lajos Hanzo (2016). "Synergistic spectrum sharing in 5G HetNets: A harmonized SDN-enabled approach." *IEEE Communications Magazine 54*(1), 40–47.

[23] GSM Alliance, "Remote Provisioning Architecture for Embedded UICC," GSM Alliance, SGP.02 v3.1, 2016.

[24] GSM Alliance, "Embedded SIM Remote Provisioning Architecture," GSM Alliance, 12FAST.13 v1.1, 2013.

[25] Palattella, Maria Rita, Pascal Thubert, Xavier Vilajosana, Thomas Watteyne, Qin Wang, and Thomas Engel (2014). "6tisch wireless industrial networks: Determinism meets ipv6." In *Internet of Things*, pp. 111–141. Springer, Cham.

[26] Rost, Peter, Albert Banchs, Ignacio Berberana, Markus Breitbach, Mark Doll, Heinz Droste, Christian Mannweiler, Miguel A. Puente, Konstantinos Samdanis, and Bessem Sayadi (2016). "Mobile network architecture evolution toward 5G." *IEEE Communications Magazine*, 54(5) 84–91.

[27] Wollschlaeger, Martin, Thilo Sauter, and Juergen Jasperneite (2017). "The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0." *IEEE Industrial Electronics Magazine, 11*(1), 17–27.

[28] Xiang, Wei, Kan Zheng, and Xuemin Sherman Shen, eds. *5G mobile communications*. Springer, 2016.

[29] Firoozjaei, Mahdi Daghmehchi, Jaehoon Paul Jeong, Hoon Ko, and Hyoungshick Kim. (2017). "Security challenges with network functions virtualization." *Future Generation Computer Systems* 67, 315–324.

[30] Fall, Kevin R., and W. Richard Stevens. *TCP/IP illustrated, volume 1: The protocols*. addison-Wesley, 2011.

[31] Stallings, William, and Moumita Mitra Manna. *Operating systems: internals and design principles*. Pearson, 2015.

[32] Almorsy, Mohamed, John Grundy, and Ingo Müller (2016). "An analysis of the cloud computing security problem." *arXiv preprint arXiv:1609.01107*.

[33] Singh, Ashish, and Kakali Chatterjee (2017). "Cloud security issues and challenges: A survey." *Journal of Network and Computer Applications* 79, 88–115.

[34] ETSI, "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance", ETSI GS NFV-SEC 003 v.1.1.1, 2014.

[35] ETSI, "Network Functions Virtualisation (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points", ETSI GS NFV-SEC 014 v0.0.15, 2018

[36] Baldini, Gianmarco, Taj Sturman, Abdur Rahim Biswas, Ruediger Leschhorn, Gyozo Godor, and Michael Street (2012). "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead."*IEEE Communications Surveys & Tutorials 14*(2), 355–379.

[37] Roh, Wonil, Ji-Yun Seol, Jeongho Park, Byunghwan Lee, Jaekon Lee, Yungsoo Kim, Jaeweon Cho, Kyungwhoon Cheun, and Farshid Aryanfar (2014). "Millimeter-wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results." *IEEE communications magazine 52*(2), 106–113.

[38] Park, Jung-Min, Jeffrey H. Reed, A. A. Beex, T. Charles Clancy, Vireshwar Kumar, and Behnam Bahrak (2014). "Security and enforcement in spectrum sharing." *Proceedings of the IEEE, 102*(3), 270–281.

[39] Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. "Meltdown."*arXiv preprint arXiv:1801.01207* (2018).

[40] Goel, Diksha, and Ankit Kumar Jain. "Mobile phishing attacks and defence mechanisms: state of art and open research challenges." *Computers & Security* (2017).
[41] 3GPP, "Study on the security aspects of the next generation system," 3GPP TR 33.899 v1.3.0, 2017.
[42] 3GPP, "Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description; Stage 2 (Release 15)," 3GPP TS 38.300 v15.0.0, 2018.
[43] 3GPP, "Technical Specification Group Radio Access Network; NG-RAN; Architecture description (Release 15)," 3GPP TS 38.401 v15.0.0, 2018.

Biographies

Anand R. Prasad, Dr. & ir., Delft University of Technology, The Netherlands, is Chief Advanced Technologist, Executive Specialist, at NEC Corporation, Japan, where he leads the mobile communications security activity. Anand is the chairman of 3GPP SA3 (mobile communications security standardization group), a member of the governing body of Global ICT Standardisation Forum for India (GISFI), founder chairman of the Security & Privacy working group and a governing council member of Telecom Standards Development Society, India. He was chairman of the Green ICT working group of GISFI. Before joining NEC, Anand led the network security team in DoCoMo Euro-Labs, Munich, Germany, as a manager. He started his career at Uniden Corporation, Tokyo, Japan, as a researcher developing embedded solutions, such as medium access control (MAC) and automatic repeat request (ARQ) schemes for wireless local area network (WLAN) product, and as project leader of the software modem team. Subsequently, he was a systems architect (as distinguished member of technical staff) for IEEE 802.11 based WLANs (WaveLAN and ORiNOCO) in Lucent Technologies, Nieuwegein, The Netherlands, during which period he was also a voting member of IEEE 802.11. After Lucent,

Anand joined Genista Corporation, Tokyo, Japan, as a technical director with focus on perceptual QoS. Anand has provided business and technical consultancy to start-ups, started an offshore development center based on his concept of cost effective outsourcing models and is involved in business development.

Anand has applied for over 50 patents, has published 6 books and authored over 50 peer reviewed papers in international journals and conferences. His latest book is on "Security in Next Generation Mobile Networks: SAE/LTE and WiMAX", published by River Publishers, August 2011. He is a series editor for standardization book series and editor-in-chief of the Journal of ICT Standardisation published by River Publishers, an Associate Editor of IEEK (Institute of Electronics Engineers of Korea) Transactions on Smart Processing & Computing (SPC), advisor to Journal of Cyber Security and Mobility, and chair/committee member of several international activities.

He is a recipient of the 2014 ITU-AJ "Encouragement Award: ICT Accomplishment Field" and the 2012 (ISC) 2 Asia Pacific Information Security Leadership Achievements (ISLA) Award as a Senior Information Security Professional. Anand is Certified Information Systems Security Professional (CISSP), Fellow IETE and Senior Member IEEE and a NEC Certified Professional (NCP).

Sivakamy Lakshminarayanan received B.E. in Computer Science and Engineering from Rajalakshmi Institute of Technology, India in 2016. She has 21 months of experience in Research and Development of mobile communication networks and security standardization. At present she works as Member Technical Staff in NEC India Standardization (NIS) Team at NEC Mobile Network Excellence Center (NMEC), NEC Technologies India Pvt Ltd, Chennai. In her current role, she is working on 5G Security. Her research interest includes Cyber Security, Telecom Security and Machine Learning.

Sivabalan Arumugam received Ph.D in Electrical Engineering from Indian Institute of Technology Kanpur, India in 2008 and M.Tech degree from Pondicherry University, India, in 2000. He has 14 years of experience in Academic teaching and Research. Presently he works as Assistant General Manager for Research at NEC Mobile Network Excellence Center (NMEC), NEC Technologies India Pvt Ltd, Chennai. Prior joining NECI he was associated with ABB Global Services and Industries Limited, Bangalore as Associate Scientist. He has published more than 25 papers in various International Journals and Conferences and also participated in many National and International Conferences. In his current role, he is representing NEC for Global ICT Standards forum of India (GISFI). His research interest includes Next Generation Wireless Networks.