Security and Privacy Aspects in 5G Networks

Nisha Panwar[1] and Shantanu Sharma[2]
[1]Augusta University, Georgia, USA. [2]University of California, Irvine, California, USA.

***Abstract*—The future mobile 5G networks are envisioned to support billions of devices, higher data rate, and omnipresent connectivity, with the help of a diverse set of technologies, *e.g.*, network densification, mMIMO, mm-Wave, full-duplex radios, network slicing, visual-light communication, cognitive radio networks, device-to-device communications, machine-to-machine communications, and satellite-based communication. While 5G will assist in a wide range of applications, heterogeneous devices and technologies impose significant threats to 5G networks as compared to the previous generation of the communication networks. In this article, we discuss the need of new security techniques for 5G networks and the key research challenges related to security/privacy in 5G networks.**

I. Introduction

More than 50 billion devices are expected to utilize the cellular network services by the end of the year 2025, and it would increase a substantial amount of data traffic. To support such an upsurge, the state-of-the-art solutions will not be sufficient. Particularly, the increase of 3D ('D'evice, 'D'ata, and 'D'ata transfer rate) requires the development of 5G networks that are perceived to realize the following three main features:

- *Ubiquitous connectivity*: In future, many types of devices will connect ubiquitously and provide 24×7 uninterrupted device connectivity, communication services, and smooth consumer experience.
- *Zero-latency*: The 5G networks will support life-critical systems, real-time applications, and services with zero delay tolerance. Hence, it is envisioned that 5G networks will provide zero-latency that is the extremely low latency of the order of 1 millisecond.
- *High-speed Gigabit connection*: The zero-latency property could be achieved using a high-speed connection for fast data transmission and reception, which will be of the order of Gigabits per second to users and machines.

Additionally, 5G networks are envisioned to excel the following new features over its predecessors: (*i*) 10-100x number of simultaneously connected devices, (*ii*) 1000x higher mobile data volume per unit of area, (*iii*) 10-100x higher data rate, (*iv*) nearly 1-millisecond overall communication latency, (*v*) 99.99% availability, (*vi*) 100% coverage (*i.e.*, truly pervasive coverage), (*vii*) $\frac{x}{10}$ lower energy consumption as compared to the year 2010 (*i.e.*, eco-friendly), (*viii*) $\frac{x}{5}$ lower network management operation expenses, (*ix*) seamless integration of the current wireless technologies, and (*x*) advanced security and privacy features. Figure 1 illustrates the features of 5G network (in the inner circle) and underlying technologies to achieve the features (in the outer circle).

In order to collectively achieve such goals, 5G networks will incorporate different technologies such as network densification (or small-cell (SC) networks), massive multiple inputs and multiple outputs (mMIMO or large-scale antenna systems), millimeter wave (mm-Wave), full-duplex radios, network function virtualization (NFV), software-defined networks (SDN), network slicing (NS), cloud-based radio access networks (C-RANs), visual-light communication (VLC), cognitive radio networks (CRNs), device-to-device (D2D) communications, machine-to-machine (M2M) communications, frequency division duplex (FDD), multi-radio access technology (multi-RAT), and satellite-based communication (SATCOM). An overview of such technologies may be found in [1].

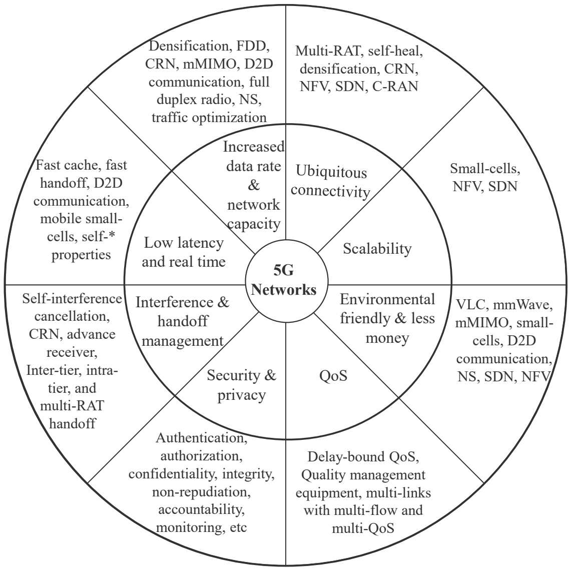
Densification, FDD, CRN, mMIMO, D2D communication, full duplex radio, NS, traffic optimization
Multi-RAT, self-heal, densification, CRN, NFV, SDN, C-RAN
Small-cells, NFV, SDN
VLC, mmWave, mMIMO, small-cells, D2D communication, NS, SDN, NFV
Delay-bound QoS, Quality management equipment, multi-links with multi-flow and multi-QoS
Authentication, authorization, confidentiality, integrity, non-repudiation, accountability, monitoring, etc
Self-interference cancellation, CRN, advance receiver, Inter-tier, intra-tier, and multi-RAT handoff
Fast cache, fast handoff, D2D communication, mobile small-cells, self-* properties
Increased data rate & network capacity
Ubiquitous connectivity
Scalability
Environmental friendly & less money
QoS
Security & privacy
Interference & handoff management
Low latency and real time
5G Networks

Fig. 1: 5G network's features and supporting technologies.

Table I presents use-case applications of 5G networks. Let us discuss one of the use-cases to see the need of secure 5G networks. **Autonomous Transportation.** Autonomous transportation will be a revolutionary use-case of 5G networks that can provide faster data transfer rate and omnipresent connectivity to autonomous vehicles. Autonomous vehicles interact with the infrastructure and neighboring vehicles for predicting road surface, traffic congestion, traffic lights, safety distance in a platoon, lane-keeping, and sharing geo-spatial statistics. These interactions provide a smooth driving and ahead of time decision making capability. For example, vehicle platooning requires that vehicles should form a group, while keeping mutual safety distance and that would: (*i*) reduce the fuel consumption because of reduced environmental friction (very similar to what birds and dolphins do in their space), and (*ii*) reduce the connection links with the infrastructure to one connection per platoon than one connection per vehicle. Note that the high-speed maneuvering requires omnipresent network connectivity and minimum latency. Such requirements can be satisfied by integrating new technologies in the communication network, *e.g.*, M2M/D2D based communication among moving cars, VLC based legitimate vehicle authentication, and SATCOM based for ubiquitous connectivity and coverage at a global scale, specifically, in a scenario where either the terrestrial communication infrastructures do not exist, or the rapid installation/deployment of the terrestrial communication infrastructures is very costly.

Now, to visualize the need of security in 5G networks, consider

978-1-7281-8326-8/20/$31.00 ©2020 IEEE

Area	**Applications and use of 5G networks**	**Benefits**
Internet-of-Things (IoT)	IoT organizes many sensors for monitoring purposes in several areas, also in the terrestrial communication infrastructure-less areas (*e.g.*, river, ocean, dams, mountains, and grids). These sensors generate a lot of data, possibly video data that needs to be transmitted to the core network and the cloud for data processing. However, this data increases network traffic. Also, deploying terrestrial networks in different types of places incurs a significant cost. The integration of 5G and SATCOM helps in such scenarios.	Reduced network traffic and reduced terrestrial networks' deployment cost.
Data distribution	During an event, many spectators use Facebook Live or similar applications that produce a huge amount of streaming data, flowed over the network. In such a scenario, instead of overburdening the entire network, the cloudification techniques can help to handle the bursty data.	Reduction in network traffic.
Emergency	Terrestrial communication infrastructures are prone to natural disasters, leaving the user without any connectivity. Here, cloud-based functions of the terrestrial communication can be reached by SATCOM.	Communication/message facility in an emergency.
High-speed systems	Currently, in non-disastrous conditions, users experience non-continues connectivity in rural areas, mountains, or high-speed trains. Also, when multiple users and sensors in a dynamic object (*e.g.*, car, train), switch from one cell to another cell, it results in bursty network traffic. Such cases can be handled by deploying small-cells.	Ubiquitous connectivity, coverage, coordinated handover, and reduced traffic.
Navigation and localization	Many government organizations/industries are interested in the end-to-end tracking of persons/vehicles, which is impossible due to the absence of terrestrial networks in many places. In this scenario, small-cells, SETCOM, and M2M communication can help.	Fine-grained global localization.

TABLE I: The use of 5G networks and its underlying technologies in different areas.

Attacks	**Purpose**	**Breaking security goals**	**Affected technology**
Existing passive attacks			
Traffic analysis and eavesdropping	Intercepting and examining messages to deduce message information, which may reveal data and communication secrecy.	Confidentiality	Any
Replay	Capturing a legal message and subsequently transmitting the message.	Authentication, integrity	Physical layer
Existing active attacks			
Jamming	Block the wireless medium by producing inference signals. This also leads to GPS jamming attacks.	Availability	Physical layer
Spoofing/Masquerading/ Man-in-the-Middle/ Session hijacking	An adversary pretends to be a legal user by blocking/stealing legal signals, IP-addresses, user IDs (*e.g.*, IMSI), or messages and establishing a false link between a legal sender and a legal receiver. This also leads to GPS spoofing attacks.	Authentication	SATCOM, SDN, Physical layer, CRN, D2D, M2M, SC
Repudiation	A denial activity of the user who had performed the task.	Non-repudiation	NFV, CRN, D2D, M2M, SC
Tampering	Changing the content of a message.	Confidentiality, integrity	Physical layer, D2D, M2M, SC
Denial-of-service (DoS)	Block the network resource to its legitimated users by message flooding.	Availability	SDN, NFV, NS, Physical layer, CRN, D2D, M2M, SC
Reflection attacks	Attack the sender by using the same authentication protocol so that the sender provides the answer to its own authentication challenge.	Authentication	Physical layer, CRN, D2D, M2M, SC
Routing table attacks	Malicious changes in the routing table, leading to use a malicious path for packet forwarding.	Authentication, integrity	SDN, NFV, NS, D2D, M2M, SC
New attacks			
Applications-based attacks (*e.g.*, Pegasus)	Installing a malware for executing man-in-middle, id-based attacks, compromising other connected devices, transferring fake data, exposing sensitive data, tracking calls, and collecting passwords.	Authentication, confidentiality, integrity	Cloud, SDN, User Equipment (UE), NFV, D2D, M2M, SC
OS attacks	Exploit mobile backup data at the mobile vendor site, unauthorized access, scan mobile data, launch an app, fraud mobile payment.	Authentication, confidentiality	UE, D2D, M2M, SC
Virtualization attacks (*e.g.*, XcodeGhost and FalseGuide)	Attacks on clouds, virtual machines, communications between different applications running on different cloud platforms, and revealing data or computations at the cloud.	Authentication, confidentiality, integrity, non-repudiation, availability	Cloud, SDN, NFV
Small-cells	Holding resources of the network, downgrade attacks via a rogue SC base station, modify, insert, and eavesdrop on user traffic, DoS, and replay attacks.	Authentication, confidentiality, integrity, availability	SC
Integration/connected techniques and components	Many new techniques are assumed to be integrated into 5G networks; hence, a small loophole in any technique may damage the network by exploiting vulnerabilities in insecure systems. Also, one user may use multiple devices, where attacking a single device may harm other connected devices, stealing sensitive data, breaking the user's privacy.	Authentication, confidentiality, integrity, availability	SATCOM, SDN, NFV, NS, CRN, D2D, M2M, SC
Social networking	These attacks focus on breaking at least one device containing user sensitive data by fake apps, plug-ins, offers, click hijacking, botnets, and impersonation.	Confidentiality	User Equipment (UE)
WiFi	Eavesdropping, message tampering by a fake access point, hotspot hijacking, leaking user sensitive information, and MAC address tracking.	Authentication, confidentiality, integrity, availability	D2D, SC, User Equipment (UE)
Channel scanning	Maliciously scanning all the channels to know the information of participants (and may launch attacks later).	Availability	Any

TABLE II: Existing and new security attacks in the context of 5G networks.

an adversary that can passively listen to the entire communication. Such an adversary can easily jeopardize user privacy, by collecting the entire data belong to a group of users' movements. Furthermore, an active adversary may, further, exacerbate the damage, by injecting false data into the communication network, and that may result in life-threatening decisions while driving vehicles. Thus, while 5G will support several future applications, the security of the network (from an end-to-end perspective) is critical. ■

Outline. §II and §III discuss the need and the challenges to design new security solutions for 5G network, respectively.

Use-cases	Fast authentication	Frequent authentication	Confidentiality	Integrity	Privacy	Availability	Accounting	Secure auditing	Latency
Communication			✓	✓	M	M	M	L	M
Handover	✓	✓	✓	✓	M	M	M	L	M
Health-monitoring			✓	✓	H	M	L	M	M
Remote surgery			✓	✓	H	H	H	H	L
Transportation	✓	✓	H	H	H	H	H	M	L
Multimedia			✓	L	M	M	L	L	L
Smart city			✓	✓	H	M	M	L	H
Smart building and home	✓		✓	✓	M	M	M	L	H
Emergency systems	✓		H	H	H	H	H	H	L
Critical system monitoring	✓		H	H	H	H	H	H	L
Smart grid	✓		H	H	H	H	H	H	M
Agriculture			M	M	M	M	L	L	H
Financial systems	✓		H	H	M	H	H	M	M
Smart shopping	✓		M	M	M	L	L	L	H
Smart factories	✓		H	H	H	M	M	L	M

TABLE III: Different 5G network use-cases and relative ranking for security and privacy. L: low, M: medium, H: high.

II. Needs of New Security Techniques

The existing communication techniques have many severe security-related pitfalls, such as spoofing, jamming, privacy breach, international mobile subscriber identity (IMSI) catching, denial-of-service (DoS) attacks, and Internet Service Provider (ISP) level threats. However, in 5G networks, the scope of these problems will be catastrophic. Table II presents existing and new security attacks in the context of 5G networks. This section discusses the major factors that require to develop a new end-to-end secure architecture for 5G networks.

Massive devices, different services, and different security levels. 5G networks will support many applications of different service requirements [2]. These services will involve different actors that demand non-identical security and privacy mechanisms into the scope. Furthermore, due to non-identical access technologies, ubiquitous connectivity, and a large number of devices, users' sensitive information (*e.g*., bank passwords, medical records, user-related data collected from sensors) may be targeted easily. For example, transportation systems require ubiquitous connectivity with fast and frequent authentication, while smart-home devices, which are relatively static, do not require fast and frequent authentication. Since a user can communicate with home devices via her car, user-related data spread to different types of devices. (Table III shows different 5G use-cases and their relative ranking for security and privacy requirements.) Hence, the new security system must keep each component safe and isolated from other components, making a compromised component would not either affect or reveal the sensitive information about other components, and thus, plug-in-based security and privacy techniques will not work in 5G network.

Privacy and trust models. In the future applications, the privacy requirements will be crucial and more focused on preventing (*i*) *user privacy* (user's location, communication frequency, identifiable user information across mobile networks), (*ii*) *network privacy* (the number of slices in the network, user handovers, the identification of virtual resources, and supported applications), and (*iii*) *device privacy* (device location, owner information, usage of devices, data and communication patterns). Preventing user privacy will be the most challenging task, since, typically, a user owns many devices, which may store user's data across multiple clouds traversing over heterogeneous network equipment. Consequently, any user-sensitive information can be scraped out of any smaller part of the network using data mining/analysis techniques [2].

Intuitively, heterogeneous devices, services, and applications have non-identical trust requirements. For example, consider a campus scenario, where employees carry their laptops and mobile devices, connecting them to WiFi. Here, the system needs to build different trust models for desktops, laptops, and mobile devices, where mobile devices may impose new threats to the entire campus network. Therefore, new trust and privacy models should be built while considering heterogeneity and risk factors [3].

Secure virtual infrastructure and network slices (NSs). The 5G network will be built on top of virtual infrastructures (*e.g*., cloud and NSs), which flexibly share a single *physical* network among different *logical* networks (*e.g*., vehicle network, smart home network, and healthcare network) based on their needs. The virtualization and NSs provide efficient utilization of the network resources, while providing desired service requirements to each logically isolated NS, which prevents other NSs to be infected by a compromised NS [3].

In order to deal with secure virtualization, we need to deal with all the attacks specific to a virtual environment. NGMN [4] has investigated some security threats against NSs, such as impersonation and denial-of-service (DoS). For example, the NS manager, who is responsible to dynamically create and destroy slice instances and load them to the physical host platform, needs to trust the platform (and vice versa) to avoid impersonation attacks. In contrast, under DoS attacks, if an adversary exploits the physical resources of a slice, then it may lead to service denial to other slices that share the same resources. Other combustible tasks require creating diverse security systems for each task and isolation mechanisms to keep NS layers securely intact from each other.

Security automation, high reliability, and availability. The growing number of connected devices and rapidly evolving threats introduce more network security challenges. The new security setting and management should be dynamic, resulting in a security technique that can be implemented based on the need for services, applications, and devices [3]. However, an increasing churn rate could impose security overheads for on-the-fly decisions.

For real-time and mission-critical applications, a highly reliable and available network is required and that is also optimized in terms of bandwidth and delay. However, rigorous security protocols, which provide substantial security and reliability, place a tradeoff between security and availability/performance/functionality. Therefore, the security solution must optimize the availability, reliability, and privacy trade-offs, simultaneously.

III. Challenges in Designing New Security Techniques

This section will discuss challenges in designing new security protocols for 5G networks.

Heterogeneous access. The heterogeneous access technologies (*e.g*., 3G, 4G, 5G, WiFi, SATCOM, SDN, M2M, D2D communications, Bluetooth, and LAN) open new ways to attack the network and user equipment (UEs) [2]. Moreover, a UE can select its downlink and uplink from two different base-stations [5] or use two different technologies, *e.g*., SATCOM for control messages transfer and terrestrial networks for data transfer. Attacking one of the channels may lead to the failure of the entire communication. Further, in a heterogeneous access medium, different networks may use different authentication protocols that will turn device authentication to be harder. Moreover, the key management for each access network may place a burden on devices and increase the computation cost, as well as latency.

Cloudification and virtualization. Cloudification allows running resource greedy applications — authentication, mobility management, advance traffic processing, load balancing, and intrusion detection — at the cloud instead of the propitiatory network. SDN, NFV, and NS are major techniques for achieving cloudification in communication systems. The current system suffers from limitations such as the manual configuration of networking services, limited flexibility in configuring, provisioning and managing of the resources, and an absence of common standards for integrating terrestrial and cloud systems, especially integrating SATCOM with clouds and terrestrial networks [6]. The use of SDN, NFV, and NS may overcome such limitations.

The clouds, however, are prone to a wide range of attacks. A malicious user/cloud can control the entire network by altering OS, software, configuration files, or data forging. The advance traffic processing incorporating deep packet inspection and traffic classification at the cloud may also breach user privacy. Further, centralized/distributed SDN controller (the central controller leads to a single point of attacks, while distributed controllers have problems in implementing privacy policies and secure data gathering), untrusted cloud environment, shared virtual environment, virtual machine isolation, migration, privacy and confidentiality, physical cloud infrastructure security, and software security are the challenges in securing a virtual network.

Energy-efficient security protocols. The simultaneous prevention of multiple attacks comes with complex cryptographic protocols. Energy-efficient 5G network protocol designs are being developed without considering security at all. Complex security protocols (*e.g*., homomorphic encryption) provide complete security, while imposing heavy computations, and hence, not considered as time and energy-efficient. These resource-intensive solutions highly impact the battery-constraint of monitoring/sensor devices. Also, while protocols specific to one type of communication (*e.g*., M2M specific — Z-Wave or ZigBee) are energy-efficient, the protocols of other types of communication (*e.g*., SATCOM protocols) are not energy-efficient, making the entire network energy-inefficient. Thus, the challenge lies in developing light-weight, energy-efficient, and secure protocols, while integrating different technologies in 5G networks.

Authentication. An upsurge in the number of devices will complicate the authentication process. In fact, the current SIM-based authentication of a device to the network will not be enough [7], because SIM provision process, which writes a unique key for each SIM, may also be attacked, diminishing the entire security and privacy of millions of UEs, irrespective of any security mechanism layered upon. Further, user authentication methods, such as passwords, patterns, and fingerprints, are not enough due to spoofing and social-engineering attacks. Also, different use-cases of 5G network will pose different challenges in the authentication process, *e.g*., the involvement of several vertical industries will pose many threats against the networks and require an efficient authentication technique in place. Also, for some devices/applications, such as a smartphone, mutual authentication will be mandatory, while it will not be mandatory for other devices, such as in smart homes. Further, the dense deployment will result in the frequent handover of devices, and thus, need fast mutual authentication algorithms.

Transparent and flexible security/privacy architecture. Due to the increasing number of (IoT) devices and generated data, a security protocol must be independent of types of devices, communications, applications, and data storage. The design of transparent protocols faces challenges due to diverse technologies, vertical vs horizontal handover, latency, QoS, service-level agreement (SLA), network flow, and computational power. For example, a device communication using terrestrial networks faces significantly lower latency than communicating through a satellite. Similarly, flexible programmable security protocols are required, leading to easy adaptation of the protocol. There exists plenty of security solutions such as spontaneous verification via challenge-response (*e.g*., Pedersen's bit commitment protocol), unique verification via user locality (*e.g*., distance-bounding methods), and extended verification based on secret negotiation (*e.g*., Transport Layer Security (TLS)); however, a trade-off between the security and latency would be a crucial deciding factor regarding these tested and tried alternatives.

Delay-aware security mechanisms and QoS. A security and privacy protocol imposes a significant amount of delay due to additional computations. (For example, deterministic encryption, which produces an identical ciphertext for more than one occurrence of a cleartext, is not secure, takes more time in data processing as compared to cleartext data processing.) QoS measures the performance of a service, such as throughput, response time, and message drop. For safety applications, a security mechanism should be very fast while achieving a guaranteed QoS. However, the current networks incur a significant delay. for example, when connecting an idle UE with the base station. Such types of tasks in the future will require much faster authentication protocols, mobility management mechanisms, and a secure auditing mechanism for checking the desired QoS/security levels. However, heterogeneous and dynamic devices with different use-cases make security vs QoS tradeoff handling to be more difficult.

Location-assisted networks. The network design and resource allocation can be improved by using location information. Further, location availability helps in load-balancing, energy-efficiency, proactive caching, long-term UE predictability. Thus, it results in a fewer number of handovers, reduced latency, and scalable architecture for different applications, such as intelligent transportation systems, intelligent multimedia streaming. However, all such benefits foist a risk to user/device privacy, since real-time applications require fine-grained location information. Designing a secure and privacy-preserving mechanism is utmost required before implementing any real-time services on top. In addition, most of the services/apps force users to disclose their locations and to trust the service. However, these services do not provide any mechanism for deleting the old data, when users disallow the service for the future.

DoS prevention and availability. As mentioned earlier, DoS attacks will broaden their scope in 5G networks. DoS attacks' prevention requires secure SCs, secure mobility management entities (MMEs), and a fast authentication mechanism; leading to higher availability of the network. However, DoS prevention in 5G networks will bring in many challenges: how to distinguish between the real and bogus data transmitted by unknown devices, how to categorize a DoS attack, and how to distinguish between a fake base-station and a real base station.

All-IP networks. The future networks are assumed to be all-IP networks, thus, all the devices in the network are addressable. This means that if a malicious device can compromise a base-station, it can further affect many devices in the network through the base-station [8] or by scanning spectrum leading to DoS attacks. Further, compromising any device may reveal all the private information, the secret encryption/decryption keys, and replacing the real device by a fake device. Thus, all-IP networks push new attack dimensions and require us to design efficient firewalls and authentication systems.

Security Challenges Specific to New Technologies. Below, we discuss security challenges due to new technologies to be included in 5G networks.

Attacks to/from small-cells. Small-cells are crucial from the perspective of achieving faster data rate, efficient spectrum usage, energy-saving, and relatively economic deployment than a physical base station's deployment. Often, a SC, which is not deployed by the trusted network, covers several people in a public area. Hence, SCs are prone to more attacks. Intuitively, a compromised SC can attack several attached UEs and the core network too. Moreover, one can explicitly deploy a malicious SC for corrupting and executing various attacks on the network and other devices [8]. Hence, there is a need to know how to differentiate trusted and malicious SCs, how does a device trust a SC, and how to keep safe a trusted SC.

D2D communication. D2D communication, often, allows proximity devices to communicate with each other without involving the base station. The independence from a base station in D2D communication makes them different from M2M communication, which involves a base station when communicating to a server. In D2D communication, a malicious device can steal sensitive data from other devices involved in the communication and thus, can break the privacy. Direct wireless communication, mobility of users, completely untrusted environment, maintaining context-based privacy, device anonymity, and proximity-based attacks using a third-party application put new challenges into the scope.

M2M or IoT communication. M2M communication, which takes place among machines/sensors or between a machine and a server, is a palpable use-case that boosts the need of 5G networks in many aspects (*e.g.*, wide-coverage, connectivity, bursty data transfer). The ease of using sensors places many challenges on the communication media in terms of high overhead, the need of a significant amount of bandwidth, and security/privacy. Since M2M communication happens in untrusted and unprotected environments, it may lead to more severe attacks such as device tracking, false data injection, data manipulation, privacy leakage, and critical infrastructure (*e.g.*, dam, grid, water pump, nuclear reactors) damage, and thus, may restrict the utility of IoT, also. Lack of technical expertise in handling sensor devices, an increasing number of sensors, weak embedded OS, maintaining anonymity, light-weight authentication protocols, secure data capturing, energy-efficient cryptographic protocols for battery-sensitive sensors, query privacy, and privacy-preserving computations are other challenges that need to be solved in the context of secure M2M communications.

CRNs. CRNs allow a cognitive radio (CR) node to learn the surrounding spectrum/channels and to make on-the-fly decisions for a channel selection that would efficiently utilize the spectrum. Here, a malicious CR node can scan many channels, leading to DoS attacks on all channels and power exhaustion of other nodes that scan the channel. CRNs imposes the following challenges: authentication of the primary/legal user of the channel, CR node authentication, and detection of a selfish user who uses channels belonging to others but never shares her channels with others.

IV. Conclusion

This article discusses the need of new security techniques and the new challenges in designing security techniques for 5G networks. Due to diverse applications, many devices, different types of communication technologies, and the desired goal of fast communication, designing an end-to-end secure 5G network will be a crucial but not a trivial task. Thus, an entangled yet interesting bunch of research directions in the context of 5G networks is open to be explored.

References

[1] N. Panwar *et al.*, "A survey on 5G: The next generation of mobile communication," *Physical Communication*, vol. 18, pp. 64–84, 2016.

[2] "5G scenarios and security design," tech. rep., Huawei, 2016. Available at: http://www-file.huawei.com/~/media/CORPORATE/PDF/white%20paper/5g-scenarios-and-security-design.pdf.

[3] "5G PPP phase1 security landscape," tech. rep., 5GPPP, 2017. Available at: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf.

[4] "5G security recommendations package #2: Network slicing," tech. rep., NGMN Alliance, April, 2016. Available at: https://tinyurl.com/y6yrvnd3.

[5] F. Boccardi *et al.*, "Five disruptive technology directions for 5G," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, 2014.

[6] R. Ferrús *et al.*, "SDN/NFV-enabled satellite communications networks: Opportunities, scenarios and challenges," *Physical Communication*, vol. 18, pp. 95–112, 2016.

[7] "How spies stole the keys to the encryption castle," tech. rep. Available at: https://theintercept.com/2015/02/19/great-sim-heist/.

[8] J. Cao *et al.*, "A survey on security aspects for LTE and LTE-A networks," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 283–302, 2014.