5G as an Enabler for Secure IoT in the Smart Grid

(Invited Paper)

Ravishankar Borgaonkar
Software Engineering, Safety and Security
SINTEF Digital
Trondheim, Norway
Email: ravi.borgaonkar@sintef.no

Martin Gilje Jaatun
Software Engineering, Safety and Security
SINTEF Digital
Trondheim, Norway
Email: martin.g.jaatun@sintef.no

***Abstract*—The use of IoT devices in the future electricity domain (known as the smart grid) has numerous benefits, such as improved reliability of the power system, enhanced functions of SCADA (Supervisory Control and Data Acquisition), improved monitoring and management of operational power grid assets, and advanced metering infrastructure. The smart grid concept relies on the integration of high-speed and reliable communication networking technologies in order to provide twofold benefits - one for the interconnection between the existing power grid and intelligent information systems, and another for enabling real-time grid monitoring via IoT devices. However, the security of IoT devices themselves is a challenge due to the trade-off between device cost and secure communication requirements. Further, current electricity grids require robust and secure wireless communication infrastructure to realize transformation to smart grids. The 5G networks are considered as an enabler for digitalization of power grids and facilitating IoT connectivity for future smart grids with several benefits such as low latency, ultra high speed, and improved reliability.However, the use of public 5G networks may introduce new types of security risks to the IoT-based smart grids infrastructure. In this paper, we analyze the security aspects of 5G security specifications released by the 3GPP standards organization from the perspective of IoT-based smart grids. In particular, we consider a smart grid scenario utilizing 5G as a wireless communication infrastructure, and present 5G benefits to several security aspects such as authentication, confidentially, integrity, resiliency, and availability. Further, we outline security risks to IoT-based smart grids originating from compromised 5G network-related infrastructure.**

I. Introduction

The smart grid is more than smart meters [1], and the true potential is not realized before independently controlled sensors and actuators (in the grid primarily breakers) are linked up to the Supervisory Control and Data Acquisition (SCADA) paradigm in a true Internet of Things (IoT).

In the electricity domain, the Distribution System Operator (DSO) needs to maintain stable operation of the grid in all possible situations, also considering increasing usage of Distributed Energy Resources (DER). Hence, the DSO needs to employ different sensors and actuators on a large scale, and this quickly evolves into what we know as the Internet of Things (IoT). Further, there is a need for wireless communication technologies in order to perform real-time monitoring of smart grid operations via exchanging data from IoT devices. The main wireless communication technologies in the context of smart grids include 3GPP (2G/3G/4G/5G cellular networks) and non-3GPP (IEEE 802.11ah, SIGFOX, and LoRa). However, 3GPP cellular technologies such as 2G, 3G, 4G, and 5G are more beneficial for smart grid scenarios due to their ability to provide wider coverage to large geographical areas.

978-1-7281-3345-4/19/$31.00 ©2019 IEEE

According to a recent EU report [2], wireless technologies in particular 5G may potentially solve some of the smart grid related challenges faced by utility companies – such as connecting a vast number of sensors and deliver ubiquitous coverage with high security and reliability. Further, 5G networks are widely considered as the main component of future smart grids as several 5GPP pilot projects funded by EU demonstrate 5G based smart grid use cases [3], [4], [5]. The 5G networks marry a new service-based architecture with advanced wireless technologies to deliver innovative business use-cases requiring low latency, high capacity, and high reliability. However, there are some security concerns related to the 5G network and its deployments for national critical infrastructures.

In this paper, we analyze the 5G security architecture proposed by the 3GPP in order to understand safe and secure adaption of 5G networks for the IoT based smart grid domain. We discuss how the 5G communication network benefits numerous IoT based smart grid applications, such as for maintenance, safety, and security operations. In particular, we consider a scenario in which IoT devices use 5G cellular networks to communicate with the smart grid operation center. Accordingly, we outline a threat model for such a scenario and present security features of 5G networks applicable for future smart grids.

The remainder of this paper is organized as follows: In section II we present relevant background information about IoT device deployments in smart grid and 5G network evolution. Section IV discusses the threat model for a smart grid when 5G is primarily used as a wireless communication medium, taking the adversary model and capabilities into account. We present 5G architectural security benefits to a smart grid scenario in Section VI. Before concluding this paper in Section VIII, we discuss potential security risks to the IoT based smart grid infrastructure from 5G network related attacks in Section VII.

II. Background

According to NIST, smart grid is defined as "a modernized grid that enables bidirectional flows of energy and uses two-way communication and control capabilities that will lead to an array of new functionalities and applications." To modernized existing grids, IoT devices and the communication technologies play an important role. In this section, we describe benefits of 5G as a communication medium, and the need of IoT devices for digitization of the exiting smart grid infrastructure.

A. 5G and the Promise of Secure Ubiquitous Communication

5G can act as a vehicle to drive the digitalization phase for industry 4.0 and assist in realizing a gigabit networked-society in the coming information age. The new service based 5G architecture will marry data collection and advanced computation techniques with billions of connected devices, thereby opening up new business opportunities with an impact on global industries and economy [6]. The use-cases of 5G typically highlights - high bandwidth, massive IoT (low bandwidth) connectivity, and possibility of extreme low latency at the edges, or combinations thereof. The 5G networks attempt to showcase a number of use-cases to critical infrastructures such as emergency services, transportation, health, telecommunication, and financial services. Most of these critical infrastructures including smart grids could be using IoT devices as a sensor to detect system fault or threats or to collect critical information.

The 5G network is an evolution of 4G and promises ultra-high wireless speed, low latency, reliability, increased capacity and flexibility to satisfy the needs of different services. At the same time, the 5G security architecture integrates 4G security and enhances the weaknesses of previous generation cellular networks. Typically, cellular network architectures are divided into two types - Radio Access Network and Core Network. In the following subsections, we briefly discuss 5G network architecture and types necessary to understand security aspects relevant for smart grids.

1) 5G Radio Access Network: The Radio Access Network (RAN) in 5G consists of end-devices (for example, mobile devices, IoT devices, connected cars, etc.) and the base stations. The advanced wireless techniques such as MIMO (Multiple Input Multiple Output) enable low-latency to ultra high-speed communication via 5G base stations, which are referred to as 5G NR in technical terms. For simplicity, we use base station terminology throughout the rest of the paper. In the context of the smart grid, the RAN enables secure connectivity to the IoT devices via the use of eSIM (embedded Subscriber Identification Module). This type of eSIM modules are used for authentication and deriving subsequent security (encryption and integrity) keys to secure wireless communication. Overall, the RAN is responsible for authentication, availability, confidentiality and integrity aspects of the 5G wireless infrastructure.

2) 5G Core Network: In 5G, the Core Network (CN) is very different than in 4G due to the use of several advanced ICT technologies such as cloud computing, network function virtualization, and programmable Software-Defined Networking (SDN). The 5G CN introduces a new Service-Based Architecture (SBA) that will enable deployment of new services much faster than in 4G by the use of cloud computing technologies. In addition, it uses edge-cloud computing techniques in which base stations will be connected to the edge-clouds directly (unlike in 4G). The edge-cloud techniques together with the SBA architecture enable Mobile Edge Computing (MEC)[1] in 5G networks. MEC enables serverless computing from the massive IoT device deployment perspective [7], thus increasing the network resiliency.

3) 5G Network Types: There are two types of 5G networks: Non-Standalone Network (NSA) and Standalone Network (SA). In NSA, the 5G network uses existing core network infrastructure and functionalities of 4G together with new 5G New Radio (NR) base stations. Whereas in SA mode, the network uses 5G base stations together with the SBA based core network architecture. In the context of the smart grid, the SA mode 5G complements the self-healing and automation requirement of smart grids.

B. The Internet of Insecure Things in smart grids

Typically smart grids offer bi-directional information flow among the several system service providers such as power generation, transmission, distribution, and utilization. For enabling such bi-directional information flow, smart grids need to use various IoT devices for the operating, monitoring, data collection, analysis, safety management and control of the grid operations [8], [9], [10], [11]. These types of IoT devices are usually deployed at power plants, distribution centers, micrograds, and end-user premises. The IoT devices enable the connectivity and provide a mechanism to exchange bi-directional information flow to the control smart grid center.

For reliable connectivity, IoT devices employ various communication technologies such as short-range type (Bluetooth, WiFi, Ultra-Wideband (UWB, Zigbee)) and long-range type (cellular networks 2G/3G/4G/5G). In this paper, we focus on the use of cellular networks, in particular, 5G for enabling secure communication for IoT devices.

There are different types of characteristics and requirements for IoT devices within the smart grid, for example, low power, low data rate, short or long-distance communication with limited storage and processing capabilities. Thus, security mechanisms used for such IoT devices vary according to their characteristics. The IoT device security (including hardware to software security) is out of the scope for this paper. However, we focus on how certain features of 5G networks can be used for improving the security of IoT devices in smart grids.

[1] Mobile Edge Computing is defined as an evolved cloud computing technique in which applications are hosted at the network edge instead of in the centralized data centers.

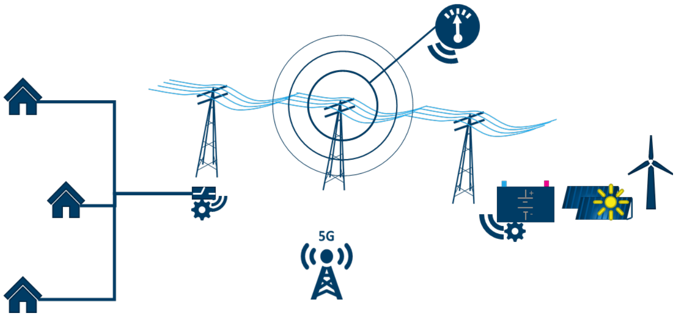

Fig. 1. Enhancing the Smart Grid with 5G

III. Related Work

In this section, we present an overview of related work in the area of 5G networks from smart grid and IoT security perspective.

Moongilan [12] and Cosovic et al. [13] investigate the use and benefits of 5G for smart grids from an electromagnetic compatibility perspective and network environment respectively. Further, Leligou et al. [14], researchers from an EU project in the 5GPP working group[2] named NRG-5, specifies how 5GPP compliant software framework benefits for energy domain and provide few such examples. In contrast, in our paper, we focus on analyzing 3GPP 5G security specifications and how these standardized methods would benefit for smart grid domain. De Dutta and Prasad [15] discuss security for smart grid in 5G and beyond networks, however, our paper outlines 5G security capabilities according to the 3GPP specification and their role in securing smart grids. Further, Kimani et al. [16] and Bekara [17] present security issues and challenges for the IoT based smart grids, whereas our paper focuses on how 5G can solve some of those challenges.

IV. Threat Model

From the perspective of the smart metering infrastructure (AMI), Tøndel et al. [18] identify the main Smart Grid assets as configuration information, identities of smart meters, control messages, meter readings, the DSO's Head End System (HES), tariffs stored in meters, and the physical meters themselves. Looking at security consequences of tighter integration between SCADA networks, distribution management Systems (DMS) and AMI, Frøystad et al. [19] identified SCADA breaker operations (i.e., the ability to control breakers in the power distribution network using SCADA), SCADA breaker status and AMI breaker operations as the primary Smart Grid information assets.

The previous two examples highlight the importance of secure communication in the smart grid. Considering the use of 5G networks in smart grids, we categorize the threat model into two types of attacks – local wireless attacks, and remote attacks against 5G or smart grid infrastructure.

In local wireless attacks, an attacker can be expected to have software and hardware capabilities to intercept or sniff wireless communication in the coverage area of 5G base stations or nearby deployed IoT devices. These types of wireless attacks can be performed either as passive or active attacks, which is analogous to the malicious adversary model used in cryptographic protocols [20]. The primary motives of the adversary against IoT devices communicating with the different network elements of the smart grid infrastructure are:

- learn the precise location of IoT devices in a given geographical area
- attempt to intercept or modify the 5G wireless communication traffic
- deny 5G wireless communication services to IoT devices.

In remote attacks, an attacker will have highly sophisticated capabilities in terms of technical knowledge and financial resources for carrying out attacks against smart grid infrastructure elements including 5G network transporting IoT data. The primary motives of the remote attackers are:

- attempt to compromise 5G network related components to steal the smart grid related critical information
- mount attacks against IoT devices via compromised 5G network elements

There are several known cases of related remote attacks against control systems in the energy sector, from Stuxnet in 2010 [21] via the Dragonfly campaign in 2014, the attacks on the Ukranian power grid in 2015 and 2016 [22], to the Triton attack in Saudi Arabia in 2017 [23]. All indicators point toward tighter integration between control networks and general ICT networks. Ridge Global [24] states that modification to the power grid should not increase the attack surface, but this is unfortunately rather optimistic. Increased functionality invariably increases the threat landscape [18].

V. Security requirements for IoT in Smart Grids

We describe the security requirements of IoT wireless communication in the context of smart grids according to the ENISA recommendation for critical infrastructure [25]. Note that we only describe wireless communication related security requirements from ENISA recommendations [25]. Related to IoT devices in all types of emergency situations, a technical report from ETSI presents requirements for a smart city use case, however, smart grids are not directly included in the standard [26].

- Authentication: IoT devices (including sensor types of devices) are required to support lightweight and mutual authentication methods. In addition, scalable key exchange mechanisms are a challenge and need to be included for subsequent security procedures such as encryption of the data.
- Privacy: The privacy of customer and system data needs to be preserved while communicating over different types of wireless technology methods.

[2] http://www.nrg5.eu/about-us-2/. The ultimate project goal is to render the deployment, operation and management of existing and new communications and energy infrastructures(in the context of the Smart Energy-as-a-Service)easier, safer, more secure and resilient from an operational and financial point of view.

- Availability: The network should provide robust and always-on connectivity to the IoT devices.
- Confidentiality: The communication protocols need to provide secure methods to ensure the confidentiality of IoT data transmitted over-the-air.
- Integrity: The over-the-air communication data needs to be integrity protected.

VI. Enabling secure IoT over 5G in Smart Grids

In this section, we consider use-case scenarios in which IoT devices within a smart grid are connected over a 5G wireless network infrastructure. According to this use-case scenario, we present benefits of 5G applicable for enabling a secure wireless communication medium in smart grids.

As shown in Figure 2, we consider two types of IoT devices:

Type A category devices are regular IoT devices, for example, connected cars, drones, etc.

Type B category devices are resource-constrained devices deployed at remote locations, for example, small wireless sensors or actuators used for temperature detection, leaning of electricity towers, etc.

The type A and B devices connect to the Smart Grid Control Center (SGCC) using 5G radio base stations via a Mobile Edge Computing Host (MECH) and the 5G Core Network. The 5G core network consists of different elements, however, these are out of scope for this paper. We describe a few elements of the core network responsible for providing security and privacy related features to the IoT devices. In particular, we mention the Authentication Server Function (AUSF), the Unified Data Management (UDM), the Network Exposure Function (NEF), the Session Management Function (SMF), and the Access and Mobility Management Function (AMF). The Smart Grid Control Center is hosted in the smart grid infrastructure and receives data via the 5G core network from the IoT devices. The interfaces I_a, I_b, I_c, and I_d among the SGSC, MECH, 5G RAN and 5G Core Network are connected as shown in Figure 2 via a private network or as specified by the 3GPP 5G security specification [27].

We present the following security benefits provided by a 5G enabled smart grid infrastructure.

A. Authentication

The 5G network provides a Universal Subscriber Identification Module (USIM), a hardware module for the use of device authentication, including IoT devices. In cellular networks, the USIM acts as a root-of-trust hardware element and can be removable or embedded in the IoT device itself. The embedded version is technically referred to as an eSIM. Such eSIM modules provide a unique way to authenticate IoT devices towards the network services and eventually to smart grid owners as well. For our smart grid scenario, the type A IoT devices can be equipped with eSIMs. In the case of type B, there could be a limitation in terms of power and system performance. However, type B small sensors may use a gateway equipped with eSIM for reporting readings or measurement data to the SGCC. In addition, similar to work presented in [28], eSIM based security solutions together with Physical Unclonable Functions (PUF) based security solutions can be used for authentication and authorization of resource-constrained type B IoT devices. The eSIM modules are widely used in today's IoT devices. According to SIMalliance, due to the fact that the eSIM provides a remote management framework, they add flexibility and control, authenticated connectivity, and dynamic security [29] (for example security credentials or algorithms can be changed remotely over-the-air).

The eSIM or removable USIM in IoT devices or gateways consist of a symmetric master key K_i. The same key K_i is also stored in the core network component AUSF, and is used to derive subsequent authentication keys for IoT devices. The authentication is performed using Authentication and Key Agreement (AKA) or the EAP-AKA protocol [27], [30]. The 5G AKA protocol is stronger than the previous version used in 4G networks, in particular, identity privacy is improved. In addition, the 5G AKA protocol provides protection against malicious wireless attacks originating from fake base stations (such attacks are possible in 4G networks [31]). However, there are a few privacy issues allowing tracking of the 5G devices [32]. The smart grid operator can utilize the eSIM remote management framework to monitor or install add-on services (for example device profiles).

In addition, the smart grid provider can use their own authentication methods in 5G networks for IoT devices instead of eSIMs such as certificates and pre-shared keys [33]. These methods could be useful for type B IoT devices in which use of eSIM would be expensive in terms of cost and technical capabilities. The 5G security standard supports EAP based secondary authentication methods between IoT devices and the external data network [27] (in our smart grid scenario for example with DSO or an actor managing IoT device types A or B via the SGCC).

B. Confidentiality and Integrity

The over-the-air (OTA) encryption is improved in 5G compared with previous generations. In our smart grid scenario context and according to the 5G security architecture [27], the OTA encryption starts from the IoT devices and terminates at the 5G base stations. Please note that the smart grid provider can utilize an additional layer of encryption for their own application, i.e., end-to-end from IoT devices to the smart grid operation center. In this paper, we focus only on the OTA encryption features and different capabilities offered by 5G networks.

The 5G network offers three variants of OTA symmetric encryption algorithms with 128-bit key size - SNOW 3G, AES and ZUC based algorithms [27]. Similarly, these three algorithms also offer integrity protection for the OTA traffic. These encryption and integrity algorithms are 3GPP standards compliant, and keys are derived from the AKA protocol used for authentication purpose and key K_i (stored in the eSIM). Both encryption and integrity protection algorithms support 128-bit key size in 5G networks. In 4G, network user traffic is not integrity protection, however, in 5G such type of traffic

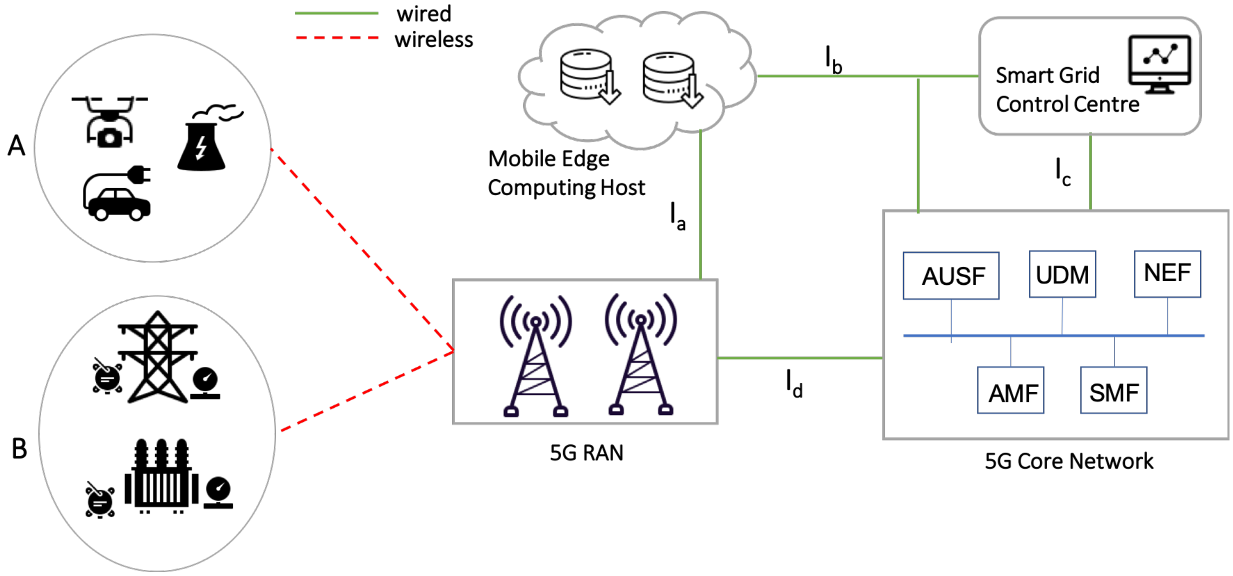

Fig. 2. 5G Use-Case : Smart Grid Scenario

(for example, feeder readings from Type A IoT devices) are integrity protected [27].

As the core network is based on SBA - network interface security between MECH to 5G RAN and MECH to SGCC can be protected using SSL/TLS [34] or IPSec [35].

C. Resiliency and Availability

According to the FP7 FINESCE project [36], [14], it is estimated that when electric vehicle penetration reaches 10% in the EU, the energy load will peak in the evenings at about 38GW, thereby introducing potential stability risks to the utilities. Leligou et al. [14] also highlight a need of ultra-fast response requirement of a communication network for smart grids specifically in the case of Phasor Measurement Unit (PMU) for fast monitoring of distribution feeders with data refresh of 10 to 50 timers per second. In addition, they point out that increasing proliferation of EVs, deployment of smart chargers and their management by DSO requires near real-time communication for vehicle to grid flexibility services. To support these low-latency and near real-time communication requirements, the 5G base station supports Ultra-Reliable Low-Latency Communication (URLLC) radio services for smart grid scenarios. Although URLLC benefits of 5G network may be realized in 5G SA mode deployments, 5G security standardization (phase 2 [37]) for URLLC services is being developed at the time of writing this paper. Further, Gustav Wikström et al. from Eicssson and ABB demonstrated how 5G URLLC can be used to provide line differential protection [38]. Their research indicates that fiber based communications used between protection units[3] can be replaced with low-latency 5G network.

In 5G SA deployment mode, a single base station can be deployed as two split units, a central and a distributed unit base station. Consequently, such a splitting method provides greater resilience against (technical or natural disaster related) failures and attacks against 5G base station specifically. The 5G security architecture supports legacy networks such as 4G, hence IoT based smart grids benefits from multi-network connectivity in terms of security and services when 5G radio is not available in some circumstances (for example DoS attacks or service disruptions). The SBA enables a network slicing feature to isolate groups of network functions from other functions in the 5G SA mode. For example, the network slice responsible for handling IoT devices within the smart grid can be isolated from other network slice serving normal 5G mobile phone traffic. Similarly, high or low-priority can be given to a particular network slice in 5G SA mode. Further, the use of software and cloud-based technologies in 5G core network enables the creation of network functions that can be scaled depending on the traffic load or isolated under the attack or network disruptions.

D. Security Standard Compliance

As compared with other wireless technologies, 5G network use 3GPP/ETSI standard compliant security protocol (such as AKA, IPsec, TLS, DTLS, etc.) and architectures. Consequently, the smart grid owner benefits from the requirement of standardized security procedures while using 5G networks.

[3] The serious damages may occur in the power grid infrastructure or to the connected consumer infrastructure (for example a factory or end-users), if there are malfunctions in the grid. Hence, it is very important and critical to timely detect faults and subsequently handle such errors in the grid. This type of detection is handled and performed by the Protection Units and line differentiation protection [38].

Although this does not resolve security and trust issues in IoT device supply chain and logistics, however, the network communication infrastructure may addresses such security issues in the upcoming 5G network due to a dedicated 5G security certification and assurance related activities in the 3GPP [39]. For example, 5G network elements such as base stations or dedicated hardware devices have to follow new 5G security certification and assurance schemes as specified by the 3GPP standard.

E. Non-Public 5G Networks

As compared with cellular networks offering services to general public users, a 5G non-public network (or also referred as private 5G networks) provides wireless network connectivity to a certain organization while deployed at their own premises, for example, factory or company premises. Such type of non-public networks are ideal for enabling connectivity and automation for Industrial IoT (IIoT) devices, according to 5G-ACIA group [4]. In the context of smart grids, such type of non-public 5G networks may be useful for energy production power plants or large-scale solar farms for collecting data from IIoT devices. For smart grid actors benefit from such non-public 5G network deployments is the isolation of IoT device traffic from public users or devices (in addition to low latency and always-on connectivity), thereby reducing threat landscape and attack vectors. However, the security of such type of Standalone 5G networks needs additional consideration on selecting the appropriate security mechanisms as outlined in the 5G-ACIA report [40].

VII. Threats originating from 5G networks

In this section, we highlight weak security interfaces of the 5G architecture and outline relevant attacks against the smart-grid infrastructure. As shown in figure 2, the 5G architecture is divided into the RAN and CN. Following threats from compromised RAN and CN may affect the smart grid:

- Though wireless security in 5G is better than in 4G, fake base station attacks[5] are still possible against devices including IoT. Shaik et al. demonstrated that fake station type of attacks are possible in 5G, compromising privacy, denial of service and draining the battery of IoT devices [41]. Similar attacks against type A and B IoT devices may be possible if these fake base station attacks are not addressed in phase 2 of the 5G security standardization process. However, such type of wireless attacks are limited due to the need for an adversary to be in the coverage area (around 1 km) of IoT devices.
- The Next Generation Mobile Network (NGMN) group indicates potential security risks associated with the MECH node and related interfaces. For example risks from user plane attacks, third party applications hosted in the MECH, storage of security sensitive data at the edge node are discussed in [42]. Hence, security misconfiguration issues at the MECH may result in affecting to the SGCC or compromising critical operational data.
-
- The 5G core network relies on securing the cloud infrastructure during the pre and post network deployment stages. The NGMN group indicates potential risks in exposing network and security capabilities of the 5G core network elements [43]. For example, in our smart grid use-case, authentication keys associated with Type A or B IoT devices could be exposed to 3rd parties via API to the 5G CN functions.

VIII. Conclusion

The IoT devices play a crucial role in transforming existing power grids into a smart grid concept. Similarly, there is a need for a secure and resilient wireless communication infrastructure to relay intelligent data from IoT devices to the smart grid operation center. In this paper, we investigate how 5G could satisfy such wireless communication requirements and present 5G security features applicable for protecting IoT based smart grids. Although 5G does not provide end-to-end security for smart grid-based applications, we present standardized 5G technical principles that can be considered while designing multi-layered security for IoT devices.

Acknowledgment

The research presented in this paper has been funded by the Norwegian Research Council through the FME Cineldi research centre, project no. 257626 (www.sintef.no/projectweb/cineldi). Thanks to Christian Frøystad for permission to re-use Fig. 1.

References

[1] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Cyber security challenges in smart grids," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Dec 2011, pp. 1–8.

[2] European Union, "5G deployment could bring millions of jobs and billions of euros benefits, study finds," Tech. Rep., 2016. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/5g-deployment-could-bring-millions-jobs-and-billions-euros-benefits-study-finds

[3] (2019) NRG5 project- enabling smart energy as service via 5G network advances. [Online]. Available: http://www.nrg5.eu

[4] (2019) WIVE project- wireless for verticals. [Online]. Available: https://wive.turkuamk.fi

[5] (2019) SONGO project- service oriented grid for the network of the future. [Online]. Available: https://www.sogno-energy.eu

[6] (2019) The 5G Economy: How 5G will Impact Global Industries, The Economy, and You. [Online]. Available: https://www.technologyreview.com/s/603770/the-5g-economy-how-5g-will-impact-global-industries-the-economy-and-you/

[7] S. Kekki, W. Featherstone, Y. Fang, P. Kuure, A. Li, A. Ranjan, D. Purkayastha, F. Jiangping, D. Frydman, G. Verin, K.-W. Wen, K. Kim, R. Arora, A. Odgers, L. M. Contreras, and S. Scarpina. (2018) MEC in 5G networks. MEC in 5G Networks. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[4] The 5G Alliance for Connected Industries and Automation (5G-ACIA) has been established to serve as the central and global forum for addressing, discussing, and evaluating relevant technical, regulatory, and business aspects with respect to 5G for the industrial domain. All relevant stakeholders take part in this initiative.

[5] In such a type of attack, a fake radio base station is used by the adversary to lure nearby radio devices to connect with the intention of stealing data or denial of service attacks. For example, low-cost fake station attack in 4G are demonstrated by Shaik et al in [31].

[8] M. Yun and B. Yuxin, “Research on the architecture and key technology of internet of things (IoT) applied on smart grid,” in *2010 International Conference on Advances in Energy Engineering*, June 2010, pp. 69–72.

[9] Q. Ou, Y. Zhen, X. Li, Y. Zhang, and L. Zeng, “Application of internet of things in smart grid power transmission,” in *2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing*, June 2012, pp. 96–100.

[10] J. Liu, X. Li, X. Chen, Y. Zhen, and L. Zeng, “Applications of internet of things on smart grid in china,” in *13th International Conference on Advanced Communication Technology (ICACT2011)*, Feb 2011, pp. 13–17.

[11] Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, “Internet of things-aided smart grid: Technologies, architectures, applications, prototypes, and future research directions,” *IEEE Access*, vol. 7, pp. 62 962–63 003, 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2913984

[12] D. Moongilan, “5G wireless communications (60 ghz band) for smart grid — an EMC perspective,” in *2016 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, July 2016, pp. 689–694.

[13] M. Cosovic, A. Tsitsimelis, D. Vukobratovic, J. Matamoros, and C. Anton-Haro, “5G mobile cellular networks: Enabling distributed state estimation for smart grids,” *IEEE Communications Magazine*, vol. 55, no. 10, pp. 62–69, Oct 2017.

[14] H. C. Leligou, T. Zahariadis, L. Sarakis, E. Tsampasis, A. Voulkidis, and T. E. Velivassaki, “Smart grid: a demanding use case for 5G technologies,” in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, March 2018.

[15] S. De Dutta and R. Prasad, “Security for smart grid in 5G and beyond networks,” *Wireless Personal Communications*, vol. 106, no. 1, pp. 261–273, May 2019. [Online]. Available: https://doi.org/10.1007/s11277-019-06274-5

[16] K. Kimani, V. Oduol, and K. Langat, “Cyber security challenges for iot-based smart grid networks,” *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36 – 49, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548217301622

[17] C. Bekara, “Security issues and challenges for the IoT-based smart grid,” *Procedia Computer Science*, vol. 34, pp. 532 – 537, 2014, the 9th International Conference on Future Networks and Communications (FNC’14)/The 11th International Conference on Mobile Systems and Pervasive Computing (MobiSPC’14)/Affiliated Workshops. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050914009193

[18] I. A. Tøndel, M. G. Jaatun, and M. B. Line, “Threat Modeling of AMI,” in *” Critical Information Infrastructures Security – Proceedings of the 7th International Conference on Critical Information Infrastructures Security (CRITIS 2012)”*, 2013, lecture Notes in Computer Science.

[19] C. Frøystad, M. G. Jaatun, K. Bernsmed, and M. Moe, “Ros-analyse ams-dms-scada – risikoanalyse av økt integrasjon mellom ams, dms og scada,” SINTEF Digital, Tech. Rep. 2018:01083, 2018. [Online]. Available: \url{http://publikasjoner.nve.no/eksternrapport/2018/eksternrapport2018_15.pdf}

[20] O. Goldreich, *Foundations of Cryptography: Volume 2, Basic Applications*. New York, NY, USA: Cambridge University Press, 2004.

[21] N. Falliere, L. O. Murchu, and E. Chien. (2011) W32.Stuxnet Dossier. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[22] A. Cherepanov and R. Lipovsky. (2017) Industroyer: Biggest threat to industrial control systems since stuxnet. WeLiveSecurity by eset. [Online]. Available: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-\-stuxnet/

[23] E. Kovacs, “New ”triton” ICS malware used in critical infrastructure attack,” *SecurityWeek*, 2017. [Online]. Available: https://www.securityweek.com/new-ics-malware-triton-used-critical-infrastructure-attack

[24] R. Watts, B. Kline, and T. Ridge. (2018) Potential electric grid vulnerability from cyber enabled foreign actors. Protect Our Power. [Online]. Available: https://protectourpower.org/wp-content/uploads/2018/11/Ridge-Global-and-Potential-Electric-Grid-Vulnerability.pdf

[25] ENISA. (2017) Baseline security recommendations for IoT in the context of critical information infrastructures. ENISA Report. [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[26] ETSI, “Study of use cases and communications involving IoT devices in provision of emergency situations,” (ETSI), TR 103.582, 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103500_103599/103582/01.01.01_60/tr_103582v010101p.pdf

[27] 3GPP, “Security architecture and procedures for 5G System,” (3GPP), TS 33.501, 2019. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/33_series/33.501/33501-f50.zip

[28] A. Cherkaoui, L. Bossuet, L. Seitz, G. Selander, and R. Borgaonkar, “New paradigms for access control in constrained environments,” in *2014 9th International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC)*, May 2014, pp. 1–4.

[29] SIMalliance. (2019) SIMs, eSIMs and secure elements. 5G Security. [Online]. Available: https://docbox.etsi.org/Workshop/2019/201906_ETSISECURITYWEEK/202106_DynamicNatureOfTechno/SESSION02_IoTDEVICESandSERVICES/SIMalliance_CRICCO.pdf

[30] J. Arkko, V. Lehtovirta, and P. Eronen, “Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA’),” RFC 5448 (Informational), Internet Engineering Task Force, May 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5448.txt

[31] A. Shaik, J. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi, “Practical attacks against privacy and availability in 4G/LTE mobile communication systems,” in *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*, 2016.

[32] Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park, and Altaf Shaik, “New privacy threat on 3G, 4G, and upcoming 5G AKA protocols,” in *The 19th Privacy Enhancing Technologies Symposium, PETS 2019*, 2019, p. To be published.

[33] K. Norrman, P. K. Nakarmi, and E. Fogelström. (2019) 5G security. 5G Security. [Online]. Available: https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system

[34] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” RFC 8446, Aug. 2018. [Online]. Available: https://rfc-editor.org/rfc/rfc8446.txt

[35] K. Seo and S. Kent, “Security Architecture for the Internet Protocol,” RFC 4301, Dec. 2005. [Online]. Available: https://rfc-editor.org/rfc/rfc4301.txt

[36] (2019) FINESEC project- integrated framework for predictive and collaborative security of financial infrastructures. [Online]. Available: https://www.finsec-project.eu/

[37] Anand R. Prasad, Alf Zugenmaier, Adrian Escott and Mirko Cano Soveri. (2018) 3GPP 5G security. [Online]. Available: https://www.3gpp.org/news-events/1975-sec_5g

[38] G. Wikström, J. Torsner, J. Kronander, O. Al-Saadeh, F. Chernogorov, G. Bag, J. Neander, K. Landernäs, and P. Hovila, “Wireless protection of power grids over a 5g network,” in *2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia)*, March 2019, pp. 976–981.

[39] 3GPP, “Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class,” (3GPP), TS 33.511, 2019. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/33_series/33.511/33511-g00.zip

[40] 5G-ACIA Group Whitepaper. (2019) 5G Non-Public Networks for Industrial Scenarios. [Online]. Available: https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-ACIA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios/5G-ACIA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios.pdf

[41] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert, “New Vulnerabilities in 4G and 5G Cellular Access Network Protocols: Exposing Device Capabilities,” in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec ’19. New York, NY, USA: ACM, 2019, pp. 221–231. [Online]. Available: http://doi.acm.org/10.1145/3317549.3319728

[42] NGMN Alliance, “5G security – package 3: Mobile edge computing / low latency / consistent user experience,” NGMN, Tech. Rep., 2018. [Online]. Available: https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2018/180220_NGMN-5G_Security_MEC_ConsistentUExp_v2.0.pdf

[43] M. ZUO, K. WANG, X. ZHUANG, M. QI, C. Hartmann, M. Kneppers, S. Yogendra, D. Rosalia, and J. Golic, “Security aspects of network capabilities exposure in 5G,” NGMN Alliance, Tech. Rep., 2018. [Online]. Available: https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2018/180921_NGMN-NCEsec_white_paper_v1.0.pdf