Received: 14 October 2020 | Revised: 14 May 2021 | Accepted: 20 May 2021

DOI: 10.1002/cpe.6466

SPECIAL ISSUE PAPER

WILEY

Improving smart grid security through 5G enabled IoT and edge computing

Ravishankar Borgaonkar[1] | Inger Anne Tøndel[1] | Merkebu Zenebe Degefa[2] | Martin Gilje Jaatun[1]

[1]Software Engineering, Safety and Security, SINTEF Digital, Trondheim, Norway

[2]SINTEF Energy, Trondheim, Norway

Correspondence
Ravishankar Borgaonkar, Software Engineering, Safety and Security, SINTEF Digital, Trondheim, Norway.
Email: ravi.borgaonkar@ieee.org

Abstract

This article investigates and analyzes the security aspects of 5G specifications from the perspective of IoT-based smart grids. As the smart grid requires high-speed and reliable communication to enable real-time grid monitoring via Internet of Things (IoT) devices, 5G can be considered a catalyst to transform the current power grid infrastructure into a smart grid. Thus, an understanding of what 5G can bring in terms of cyber security in IoT-based smart grids is important for design decisions and future risk analysis efforts. In this article, we explore a smart grid use case on automatic voltage control—a use case utilizing 5G as a wireless communication infrastructure with edge support. We identify the benefits 5G brings to several security aspects, and show how 5G security techniques are applicable to the smart grid, thus providing a foundation for future security analysis of 5G enabled smart grid systems. Future research should extend this work to additional smart grid use cases.

KEYWORDS

5G, computing, edge computing, IoT, security, smart grid

1 | INTRODUCTION

The electric power grid is a critical part of any national critical infrastructure, as it plays a vital role in the functioning of modern societies. Researchers and energy companies worldwide are exploring concepts to turn the current power grid into a smart grid infrastructure, with the overall goal of reducing greenhouse gas emissions.

The use of IoT devices in the future electricity smart grid infrastructure has several benefits, such as improved reliability of the power system, enhanced Supervisory Control and Data Acquisition (SCADA) functions, 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 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. 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 SCADA paradigm in a true Internet of Things (IoT). However, IoT systems also bring new challenges to the smart grid domain—an immature ecosystem with a diverse set of standards in terms of using proprietary cloud services, communication protocols, authentication modules, and operating systems;[2] and security concerns due to the trade-off between device cost and performance. Besides, current electricity grids require robust and secure wireless communication infrastructure to realize transformation to smart grids.[3] In fact, according to Islam et al.,[4] the IoT devices of a smart grid are identified as the weakest link in the network, since they can be compromised by the adversary in order to gain system access and to carry out further attacks.

The 5th Generation (5G) cellular networks are considered an enabler for digitalization of power grids; facilitating IoT connectivity for future smart grids with several benefits, such as low latency, ultra high speed, and improved reliability. According to a recent EU report,[5] 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 delivering ubiquitous coverage with high security and reliability. Furthermore, 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.[6-8] In addition, the 3GPP investigates 5G smart grid projects for the next release of cellular network standards.[9]

The 5G networks marry a new service-based architecture with advanced wireless technologies to deliver an environment for deploying Multi-Access Edge Computing (MEC) based applications.[10] The general assessment is that, with its evolution of machine-type communications and the concept of mobile edge computing, the emerging 5G mobile cellular network provides an adequate environment for distributed monitoring and control tasks in smart grids.[11] Nevertheless, there are few studies in the reviewed literature investigating the reliability of the 5G communication system for smart grid applications. For example, Zerihun et al.[12] have analysed how power system state estimators for Wide Area Monitoring Systems depend on 5G based communication infrastructure by using external effects such as rain and probabilities of component failure. However, from a cyber security aspect the number of investigations is still limited.

The objective of this article is to contribute to a better understanding of how 5G network technology can benefit security of IoT devices and communication within the smart grid. In order to investigate the role of 5G, we analyse a smart grid use case that has need for a massive amount of IoT devices* and communication, and where 5G connectivity will likely be important to realize the use case. The smart grid use case concerns voltage regulation, a main enabling technology in electric power grids,[14] and it involves coordination between two key roles: the Transmission System Operator (TSO), and Distribution System Operators (DSOs). Inclusion of more Distributed Energy Resources (DER) such as wind farms and solar photovoltaic farms, battery storage, electric vehicles, and so forth, puts new demands on voltage regulation. This smart grid use case is thus important to solve in order to be able to integrate DERs into the electric power grid at a larger scale.

In this article, we use the voltage regulation use case as a basis for characterizing IoT devices and identify key security requirements. Through using this realistic case for our analysis, we ensure identification of realistic challenges, and we consider to what extent they can be mitigated with 5G technology. We present a threat model related to the use cases, show how 5G connectivity can support the use case, and present how 5G network security features, according to the released 3GPP standard, can support the needs of this smart grid use case.

Our contributions in this article are summarized as follows:

- We present a smart grid use case that highlights the benefits of using 5G for communication with connected IoT devices
- We present a threat model of the use case that highlights important security challenges
- We discuss potential new threats that are introduced from the 5G infrastructure itself.

The remainder of this article is organized as follows: In section 2, we present relevant background information about IoT device deployments in smart grid and 5G network evolution, together with related work considering 5G and security in smart grids.

We present a smart grid reactive power management use case and relevant IoT deployments in Section 3. The security requirements for IoT devices in smart grid are presented in Section 4, and a threat model is outlined. The 5G architectural security benefits in the smart grid use case are presented in Section 5, and this is contrasted with some potential 5G-specific security risks to the IoT based smart grid infrastructure in Section 6. We discuss our findings in Section 7, and offer concluding remarks in Section 8.

2 | BACKGROUND

The technology behind the Smart Grid is tightly interwoven with the Internet of Things concept and (increasingly) wireless communication technologies. In this section, we present necessary background information and related work on the Smart Grid, IoT devices, and 5G technology concepts.

2.1 | Smart grid

The modernization of the electric power grid, commonly termed smart grid, impacts the whole value chain from generation to transmission and distribution, and even into the homes.[15] It is characterized by increased observability and controllability throughout the power grid,[15] made possible with increased communication capabilities and intelligence, for example, in form of sensors.[16,17] The key drivers for smart grid have been identified by

*In Norway, a country of about 5 million inhabitants, there are more than 140 000 MV/LV transformers,[13] and there could easily be 10 IoT devices associated with each.

IEC[15] to be increased usage of renewable energy resources, sustainability, competitive energy prices, security of supply and an ageing infrastructure and workforce. In this article we focus mainly on the increased usage of renewable energy resources.

With the introduction of renewable energy resources, the demands on the power grid change. Many of the renewable energy resources are less stable than their traditional counterparts, in that one cannot control when, for example, wind and solar power are available. Their location is also often different than the traditional situation where power is generated at power plants to be distributed via the power network towards the loads using a one-directional power flow. Instead, generation is distributed throughout the whole grid, as can be seen in Figure 1. Key trends include increasing amounts of *prosumers* (acting as both *pro*ducers and con*sumers* of energy) with home photovoltaic (PV) systems and batteries, increasing amounts of medium-scaled distributed generation, such as smaller wind farms and solar PV farms, and increasing demand for electricity such as high-power charging of electric vehicles and ferries. The added energy storage capacities, and many of the added energy generation systems and loads as well, can be considered to be flexible resources from an energy management point of view, as they increase the capacity of the system to change the power supply and demand when needed. As an example, pricing signals can be used to influence when consumers decide to charge their electric vehicles, and the batteries of these vehicles can even be used as a power source in the network.

The power system is traditionally divided into the following areas:

- Generation: the generation of energy, traditionally done at a power plant.
- Transmission: transmission of energy over longer distance, using high voltage
- Distribution: transmission of energy towards consumers, using lower voltage
- Load: the consumption of energy

The Transmission System Operator (TSO) is responsible for the transmission network, including overall grid stability. Each Distribution System Operator (DSO) is responsible for the distribution system in a given geographical area. With the introduction of more flexible resources throughout the grid, the TSO has the opportunity to use these flexible resources in ensuring grid stability. However, these flexible resources are not necessarily under the control of the TSO. This leads to a need for increased coordination and thus an increased need for reliable communication, distributed monitoring, and control.

The increased integration of the communication network technologies to the power system infrastructure opens the possibility for greater observability and for use of resources in an optimally coordinated way. For example, traditionally, voltage regulation (i.e., maintaining the voltage level within the acceptable window) is carried out by using components in the network which inject or absorb reactive power by taking into consideration the voltage measurements at their respective connection points. These components include On Load Tap Changers (OLTC), Flexible AC Transmission Systems (FACTS), capacitor banks, converters interfacing Renewable Energy Systems (RES) such as wind and solar generation units, converters interfacing battery storage systems, Automatic Voltage Regulating (AVR) systems of big or small scale generators (such as Distributed Generating (DG) units), voltage boosters, series reactors, and others.

With the integration of IoT enabled sensors and measuring instruments with the aforementioned components, and with the deployment of the 5G communication system, one can envision the realization of the smart grid concept with advanced observability and optimized operation. The optimized operation of the system is achieved through coordinated decision making of the setpoints for the local controllers of the components. These setpoints in general are reference signals sent to the local controllers of the components. With the perspective of our voltage regulation use case (as discussed in Section 3), the setpoints are either the reference voltage levels to be maintained at the connection point, or the amount of reactive power to be absorbed or injected by the components.

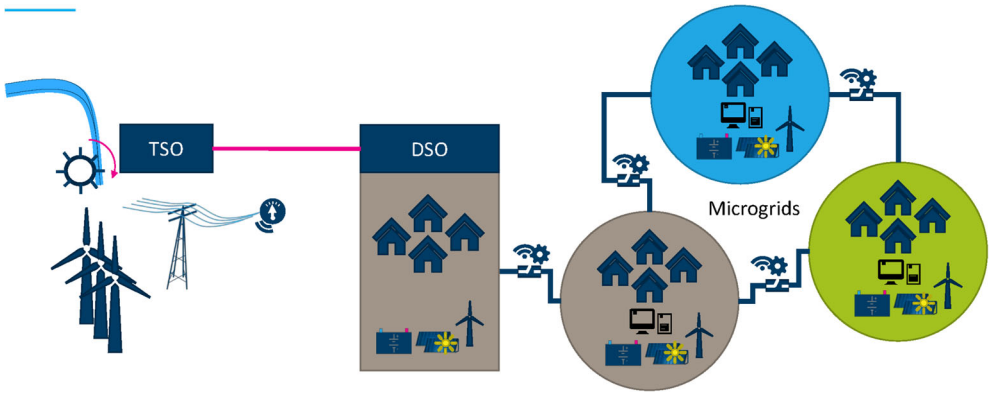

FIGURE 1 Overview of smart grid with flexible resources and microgrids

2.2 | 5G and the promise of secure ubiquitous communication

5G can act as a vehicle to drive the digitalization phase for industry 4.0,[18] and assist in realizing a gigabit-networked society in the coming information age.[19] The use cases of 5G typically highlight needs for high bandwidth, massive IoT (low bandwidth) connectivity, and possibility of extremely 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 sensors to detect system faults or threats, or to collect critical information.

The 5G network is an evolution of 4G with increasing usage of virtualization and softwarization based approaches for managing the network resources and services. At the same time, it integrates 4G security and mitigates the weaknesses of previous generation cellular networks. Typically, cellular network architectures are divided into two types—radio access network and core network. Below, we briefly discuss the different elements of the 5G network architecture necessary to understand security aspects relevant for smart grids.

The **radio access network (RAN)**[20] in 5G consists of end-devices (e.g., mobile devices, IoT devices, connected cars, etc.) and the base stations. 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 New Radio (NR) in technical terms. For simplicity, we use the base station term throughout the rest of the article. 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), which is 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.

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).[20] 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 Multi-Access Edge Computing (MEC)[†]. The MEC enables serverless computing from the massive IoT device deployment perspective,[10] thus increasing the network resiliency.

There are **two types of 5G networks**: Non-Standalone Network (NSA) and Standalone Network (SA).[21,22] 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.

2.3 | 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.[23-26] These types of IoT devices are usually deployed at power plants, distribution centers, microgrids, and end-user premises. The IoT devices enable the connectivity and provide a mechanism for bi-directional information flow to the smart grid control center.

For reliable connectivity, IoT devices employ various communication technologies of both the short-range type (Bluetooth, WiFi, Ultra-Wideband (UWB, Zigbee)) and long-range type (cellular networks 2G/3G/4G/5G). In this article, 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. IoT device security (including hardware and software security) is challenging due to trade-off between cost and resource availability, lack of security standards, and intrinsic vulnerabilities.[27] In this article, we focus on how certain features of 5G networks can be used to address some of these challenges and to improve security of IoT devices for smart grid scenarios (as illustrated in Figure 2).

2.4 | Related work in smart grid security and realization of 5G networks

In this section, we present a brief overview of related work in the area of 5G networks from a smart grid and IoT security perspective, and show how this article differs from previous efforts.

[†]Multi-Access 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[10] in 5G networks.

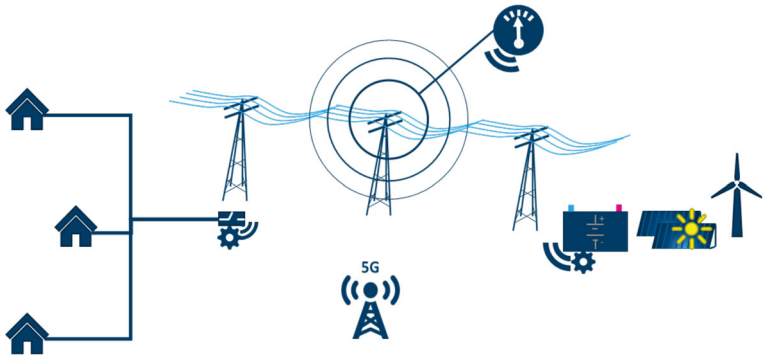

FIGURE 2 Enhancing the smart grid with 5G

In the context of 5G relation to smart grids, several studies indicate benefits of 5G network technologies to the smart grid domain. The examples include using 5G for Smart Grid Inter-Substation Control Signaling,[28] for distributed monitoring and control in smart grid,[29] and for Time Critical Communication in Smart Grid.[30] There is also an EU project on 5G Smart Grid Self-Healing Use Case.[31] Moongilan[32] and Cosovic et al.[11] investigate the use and benefits of 5G for smart grids from the perspective of electromagnetic compatibility and network environment, respectively. Further, Leligou et al.,[33] from the NRG-5 project in the 5GPP working group[‡], specify how a 5GPP compliant software framework benefits the energy domain, and provide a few such examples. Cosovic et al.[11] suggest how 5G technologies (such as mobile edge computing) benefit advanced distributed state estimation methods in future smart grids, and Zerihun et al.[12] demonstrate the effect of communication failures on state estimation in 5G-enabled smart grids. Pliatsios et al.[20] discuss realization of 5G networks. Saghezchi et al.[34] discuss directions towards a secure network architecture for smart grids in future 5G networks. In contrast, in our article, we focus on analyzing 3GPP 5G security specifications and how these standardized methods would benefit the smart grid domain.

In the area of smart grid security, El Mrabet et al.[35] provide a survey of cyber-security state and future challenges to be considered. Further, Gunduz et al.[36] highlight cyber security threats and solutions for smart grids. The communication security in smart grid is equally important, and Islam et al.[4] provide an overview of physical layer security to smart grid components. The vulnerabilities to SCADA systems including protocols is presented in a survey by Pliatsios et al.[37] De Dutta and Prasad[38] discuss security for smart grid in 5G and beyond networks, however, our article outlines 5G security capabilities according to the 3GPP specification and their role in securing smart grids. Further, Kimani et al.[39] and Bekara[40] present security issues and challenges for IoT based smart grids, whereas our article focuses on how 5G can solve some of those challenges.

3 | SELECTION OF A REALISTIC SMART GRID USE CASE: TSO-DSO REACTIVE POWER MANAGEMENT

This article makes use of a realistic smart grid use case for the purpose of analyzing and better understanding the potential role of 5G technology when it comes to security of IoT devices and communication in the smart grid. In selecting a use case we used the following criteria:

- The use case should be central for the operation of the smart grid
- The use case should involve a large amount of IoT devices
- 5G should be a relevant communication technology
- There should be the potential for serious consequences in case the use case was not performed as intended, for example, because of a cyber attack.

In power systems, reactive power plays a crucial role in regulating the voltage levels at different locations in the power network, effectively determining the power flows. Reactive power is a pulsating power which results when AC voltage is applied to capacitive, reactive loads or power electronic devices. For reactive power to exist, the waveform of the AC voltage and the current need to be out of phase. Examples of inductive loads include rotating machinery and transformers which can absorb reactive power where the current waveform lags the voltage waveform. This is due to the inductances of the windings (coils) in these devices. For example, Onload Tap Changers (OLTCs) can regulate the reactive power, and hence the

[‡]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.

voltage, by changing the number of coils in the transformers they are controlling. Capacitive loads include power system cables and capacitor banks that inject reactive power where the current waveform leads the voltage waveform. Power electronic devices such as converters of wind turbines can inject or absorb reactive power by changing the voltage/current wave forms.

Large generating units serve as sources or sinks of reactive power helping to maintain the voltage level in the network. Nevertheless, with the increasing number of distributed generators in the power system, large conventional generators such as coal power plants are decreasing. In addition, these distributed generating units such as wind turbines and solar panels are also responsible for the fast-changing voltage levels due to their intermittent infeed. To maintain the required voltage levels, TSOs are looking for alternative reactive power resources such as Renewable Energy Resources (RES) and Distributed Energy Resources (DER) in the distribution grid. However, for the TSOs to be able to tap into these resources, increased operational level collaborations are required between the TSO and the DSOs.

Khavari et al.[41] provide a use case that addresses these issues by which TSOs and DSOs collaborate for an improved power/voltage management scheme at the interface level. The use case includes evaluation of available reactive power resources to be used both in transmission grids for counteracting voltage violations caused by RES, and in distribution grids increasing RES hosting capacity. For the implementation of such a use case, a communication infrastructure is required between the TSO control room and DSO control room, also covering the sensors and controllers deployed in their respective networks. In the use case, the DSO declares the flexibility potential in its own area, and the TSO computes the optimal reactive power exchange between the TSO and the DSO. In the background, both the TSO and the DSO control rooms compute optimal setpoints for the reactive power resources in their respective areas. A high-level sketch of the system is illustrated in Figure 3.

For every power system ancillary service, such as voltage regulation, there are quality requirements from the communication infrastructure.[42] These qualities can be expressed as latency, bandwidth, reliability, and security. The required reaction time for voltage control is within the range of 2 minutes due to the electromechanical limitations of the tap changer.[43] Hence, latency in the communication infrastructure is considered to be less of a hindrance to voltage control service. Also, with the limited number of controllers and sensors that are deployed, bandwidth can be less of a problem for communication infrastructure not crowded by other services. Nevertheless, the security of the communication infrastructure can be a big concern as unwanted changes in the measurements of the sensors as well as the set points to be sent to the controllers of reactive power resources may lead to serious problems, even blackouts.[44-46] These communication security issues can be experienced as availability problems (with DoS attacks), integrity problems (with measurement and setpoint alterations), or as confidentiality problems (where the grid models are accessed by adversaries).

Without considering the state estimation related measurement sensors, voltage control services may involve actors such as Load and generation forecasting unit, TSO Optimal Power Flow (OPF), TSO SCADA/state, TSO OLTC, FACTS, DSO OPF, Power compensation units, Generator controllers,

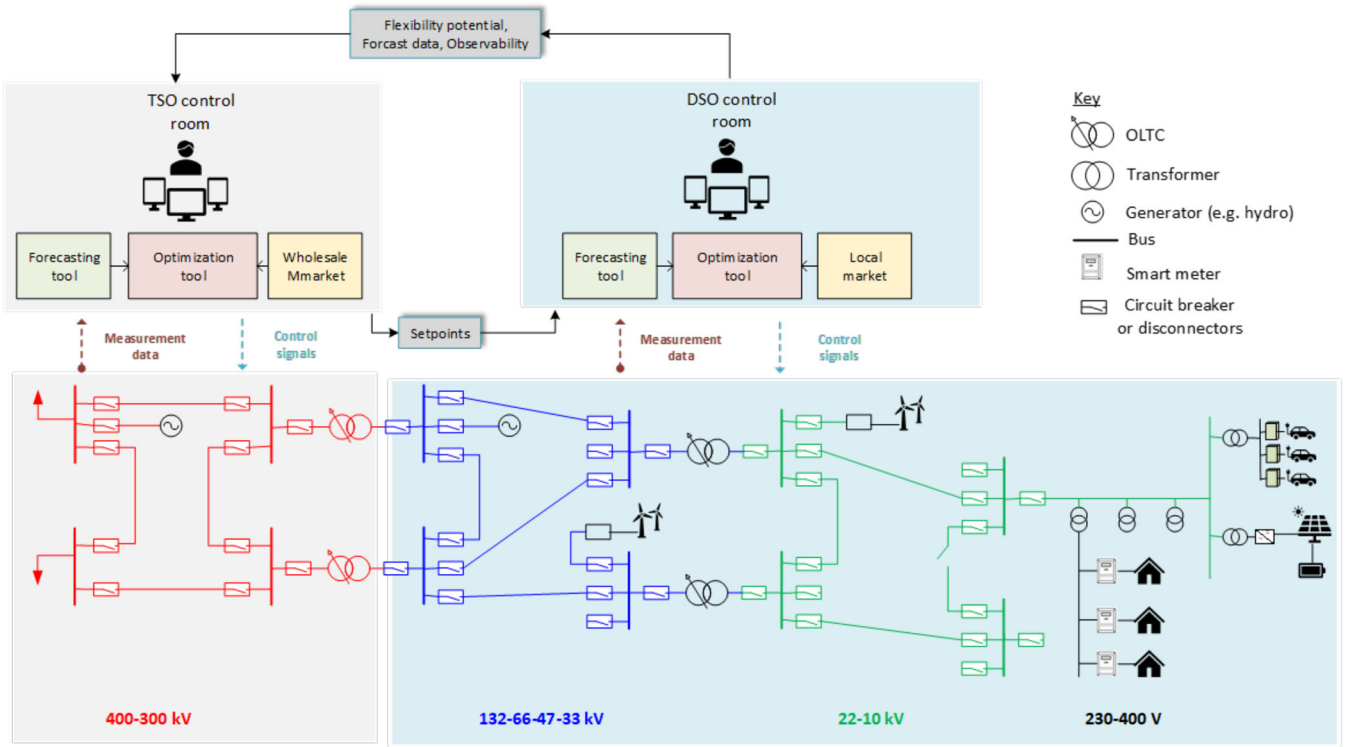

FIGURE 3 TSO-DSO coordination for activation of flexibility

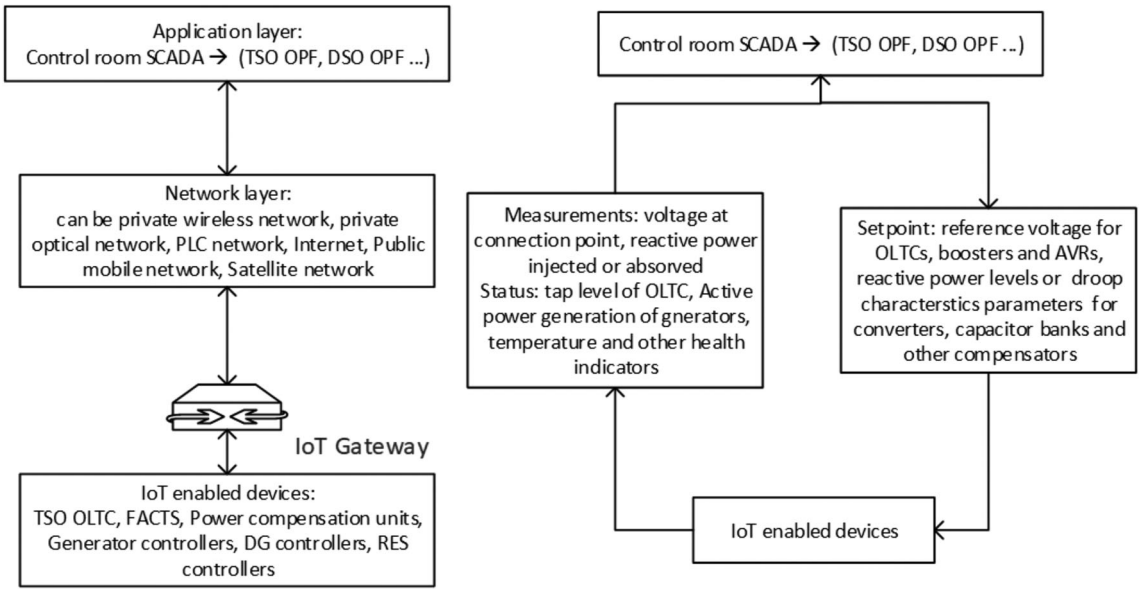

FIGURE 4 IoT layers, things and communicated measurements and setpoints

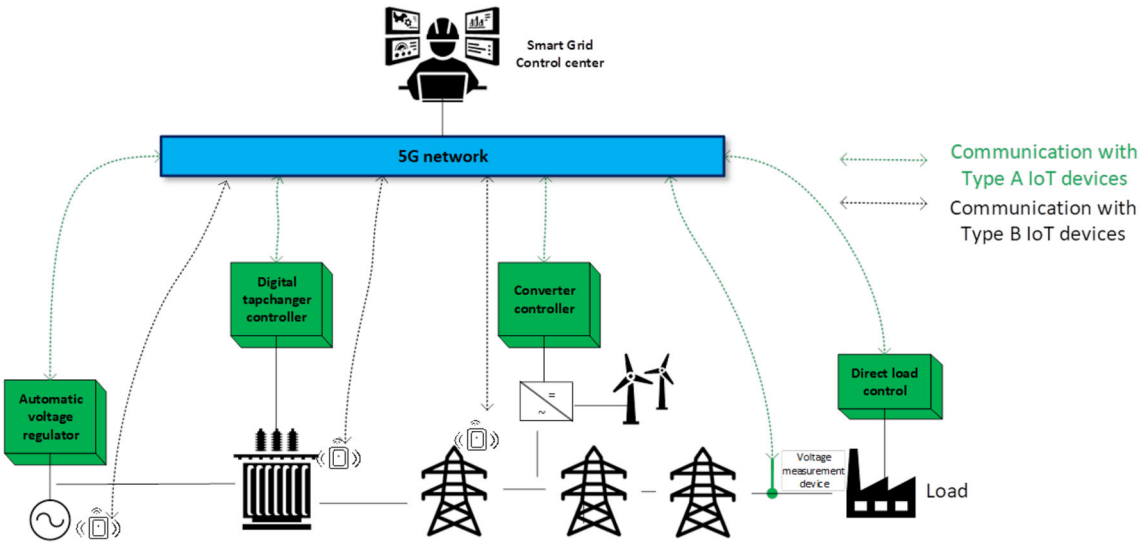

FIGURE 5 Communication of Type A and B IoT devices in the use case of voltage control

DSO DG, and RES local controllers. The measurement and status signals from the devices ('things') and the control setpoint signals sent back to them are highlighted in Figure 4, whereas in Figure 5 the IoT based architecture of the use case is illustrated in a simplified network diagram.

4 | ANALYSIS OF SECURITY REQUIREMENTS AND THREATS

In this article we consider threats towards the selected smart grid use case on TSO-DSO reactive power management. We do this by first giving an overview of relevant security requirements, at a high level. Then we present a threat model of the use case. There is a large number of articles describing and categorizing cyber security threats and attacks towards smart grid infrastructure. Wang and Lu[47] and El Mrabet et al.[35] both survey computer security in the smart grid and highlight challenges, where the latter builds on the former. Liu et al.[48] also discuss privacy risks in the smart grid. Bekara[40] and Kimani et al.[39] discuss cyber security challenges for IoT-based smart grid networks. Gunduz and Das[36] discuss smart grid treats and solutions, whereas Tøndel et al.[49] introduce a number of relevant misuse case scenarios that highlight new threats in the evolving smart grid. Otuoze et al.[50] look into where the smart grid threats originate from. These and other references can be consulted for a general overview of the

myriad of potential threats and vulnerabilities related to smart grid, as well as for an overview of known attacks. Threats and attacks that affect SCADA systems are comprehensively discussed by Pliatsios et al.,[37] who identify vulnerabilities of the associated network protocols.

4.1 | Security requirements

Among the various publications covering cyber security requirements for the smart grid in general, some examples are the ENISA recommendation for critical infrastructure,[2] the NIST guidelines for smart grid cyber security[51] and the already mentioned research articles by Wang and Lu,[47] El Mrabet et al.[35] and Gunduz and Das.[36] In this article we build on the ENISA recommendation for critical infrastructure,[2] and focus on the following wireless communication related security requirements:

- *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.
- *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.

These requirements are important in order to be able to secure the main information assets related to the smart grid. These assets include readings of voltage, current, temperature, and so forth, that are collected by IoT devices or sensors and transmitted to the control center. It also includes control signals towards IoT devices.

In this article we do not cover threats towards the IoT devices themselves (hardware and software), as we focus on the communication network and the potential role of 5G. For requirements related to IoT in a smart city use case see, for example, documentation from ETSI.[52] Note, however, that it is important to consider the varying capabilities of IoT devices.

In this article we divide IoT devices into two main types, as shown in Figure 7sz and 5. The classification of IoT devices into two groups is based on the requirements of reliable long-distance connectivity, energy consumption, and deployment cost. For example, adding 5G connectivity to every IoT device requires the addition of a modem to the hardware, potentially increasing cost and energy consumption. Hence, we assume that some IoT devices may utilize other wireless technologies (such as Zigbee or Bluetooth) to transmit data to an IoT gateway[26] equipped with a 5G modem.

Type A category devices are regular IoT devices; for example, automatic voltage regulator, digital tapchanger controller, converter controller, direct load control and so forth. These devices are usually equipped with a 5G radio modem for network connectivity.

Type B category devices are resource-constrained devices deployed at remote locations; for example, small wireless sensors or actuators used for temperature measurement, or measurement of inclination of electricity towers and transformers. In particular for this type of devices, there will be a gateway equipped with a 5G radio modem which is responsible for collecting data from the resource-constrained IoT devices.

4.2 | Threat model for 5G-enabled smart grid use case

Overall, potential attacks can be divided into the following types: local attacks requiring physical access, wireless attacks, and remote attacks. In *local attacks*, an attacker with physical access can have the capabilities and resources to physically access the smart grid infrastructure, for example, IoT devices, to modify software and hardware. In *wireless attacks*, the attacker resides in the serving area of the 5G base station without requiring physical access to IoT devices to perform attacks. The 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 type A and B 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.[53] In *remote attacks*, an attacker will have highly sophisticated capabilities in terms of technical knowledge and financial resources for carrying out attacks against IoT type A devices equipped with a 5G modem, including the 5G radio network transporting IoT data. In this article, we only consider local wireless attacks and remote attacks.

The primary motives of the adversary in local wireless attacks against IoT devices communicating with the different network elements of the smart grid infrastructure, include to learn the precise location of IoT devices in a given geographical area, to attempt to intercept or modify the 5G wireless communication traffic, or to deny 5G wireless communication services to IoT devices.

The primary motives of the remote attackers include to attempt to compromise 5G radio or core network related components to steal smart grid related critical information and mount attacks against IoT devices via compromised 5G network elements. For example, remote attacks against all type A IoT devices can result in grid instability, while control over a compromised Digital Tapchanger Controller (as shown in Figure 5) can result in a blackout scenario in the smart grid.

There are several known cases of related remote attacks against control systems in the energy sector, from Stuxnet in 2010[54] via the Dragonfly campaign in 2014, the attacks on the Ukrainian power grid in 2015 and 2016,[55] to the Triton attack in Saudi Arabia in 2017.[56] All indicators point toward tighter integration between control networks and general ICT networks. Some pundits[57] may state that modifications to the power grid should not increase the attack surface, but this is unfortunately rather optimistic. Increased functionality invariably increases the threat landscape.[58]

To build a threat model, we have used the threat modeling approach suggested by Microsoft.[59,60] We modeled the system with a Data Flow Diagram (DFD), as can be seen in Figure 6. Then we used the STRIDE mnemonic (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) to identify the main threats towards the system. STRIDE is related to the security requirements in the following way: *Spoofing* is a threat that is possible due to weak or missing authentication. *Tampering* is an attack on the integrity of the information. *Repudiation* is related to all requirements in some sense, as it is a threat to the ability to hold someone responsible for an attack that violates the security requirements. *Information disclosure* represents threats to confidentiality and privacy. *Denial of service* represents threats to availability. *Elevation of privilege* concerns attackers elevating their access rights, thereby being able to potentially violate any of the listed security requirements.

We have employed STRIDE on each trust boundary, looking at data flows that cross that boundary. Thus, our threat model is communication-centric by design. In Figure 6, we have identified three trust boundaries; between Control Room and IoT Gateway (marked ①), between IoT Gateway and "Third-party services" (marked ②), and between IoT Gateway and DG controller (marked ③). The third-party services can be cloud services, a vendor, other IoT GWs, or other IoT devices not part of this installation (threats from IoT GW towards other systems (e.g., vendor) are considered out of scope). We also assume that being able to read the value of setpoints will not be of value to an attacker. The results are summarized in Table 1.

An attack scenario for the presented use case in Section 3 can be an intruder altering the voltage level at the end of the feeder (electric transmission line) supplying a load. Let's say the attacker reduced the voltage reading at the end of the feeder to a level that is perceived by the control room as undervoltage. The optimal reactive power resources management system will compute the tap settings at which the perceived undervoltage is alleviated. The result will be, as the on-load tap changer increases the voltage, the actual voltage at the end of the feeder increases to the point of severe overvoltage, causing a total blackout. The same blackout condition can be created by a concerted effort where the setpoints of voltage regulating devices are set to a point where they all induce overvoltage. This could be achieved by, for example, manipulating the setpoints as they are communicated from the control room (trust boundary ① in Figure 6) or from the IoT GW (trust boundary ③). More attack (or misuse case) scenarios are described by Tøndel et al.[49]

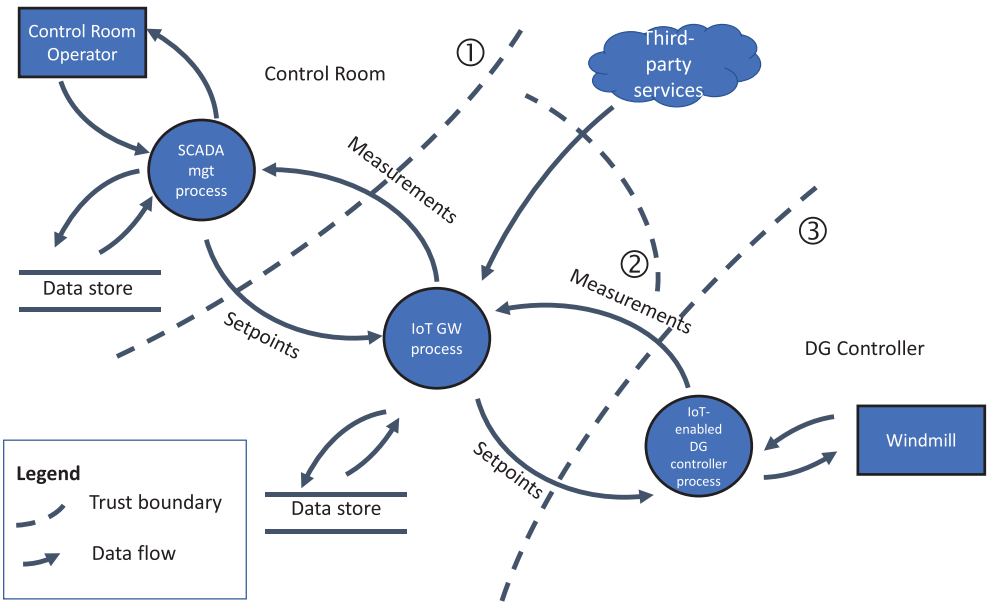

FIGURE 6 Data flow diagram for the reactive power use case

TABLE 1 STRIDE applied to the three trust boundaries ① – –③

	①	②	③
Spoofing	Spoofing of SCADA management process (to be able to submit false setpoints). Spoofing of IoT GW process (to send false measurement values).	Spoofing of vendor (to make malicious updates to GW), spoofing of Cloud/IoT GW to get data.	Spoofing of IoT GW process (to be able to submit false setpoints). Spoofing of DG controller process (to send false measurement values).
Tampering	Change setpoints or measurements.	Tamper with configuration data from vendor. Tampering with data submitted to Cloud/other IoT GW.	Change setpoints or measurements.
Repudiation	Lack of logging, cannot detect cause of incident.	Lack of logging, cannot detect cause of incident.	Lack of logging, cannot detect cause of incident.
Information disclosure	Get access to measurements from IoT devices.	Access to measurements.	Get access to measurements from IoT devices.
Denial of service	Jamming, buffer overflow.	Jamming, DDoS, buffer overflow	Jamming, buffer overflow.
Elevation of privilege	Gain administrator access at IoT GW process. Attack SCADA (gain access) via IoT GW.	Gain administrator access at IoT GW process.	Gain administrator access at IoT GW process. Attack DG Controller (gain access) via IoT GW.

5 | ENABLING SECURE IOT OVER 5G IN THE SMART GRID USE CASE

The type A and B devices connect to the Smart Grid Control Center (SGCC) using 5G radio base stations via a Multi-Access Edge Computing Host (MECH) and the 5G Core Network. The 5G core network consists of a number of different elements; however, most of these are out of scope for this article. 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 7) via a private network or as specified by the 3GPP 5G security specification.[61]

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

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, small type B sensors may

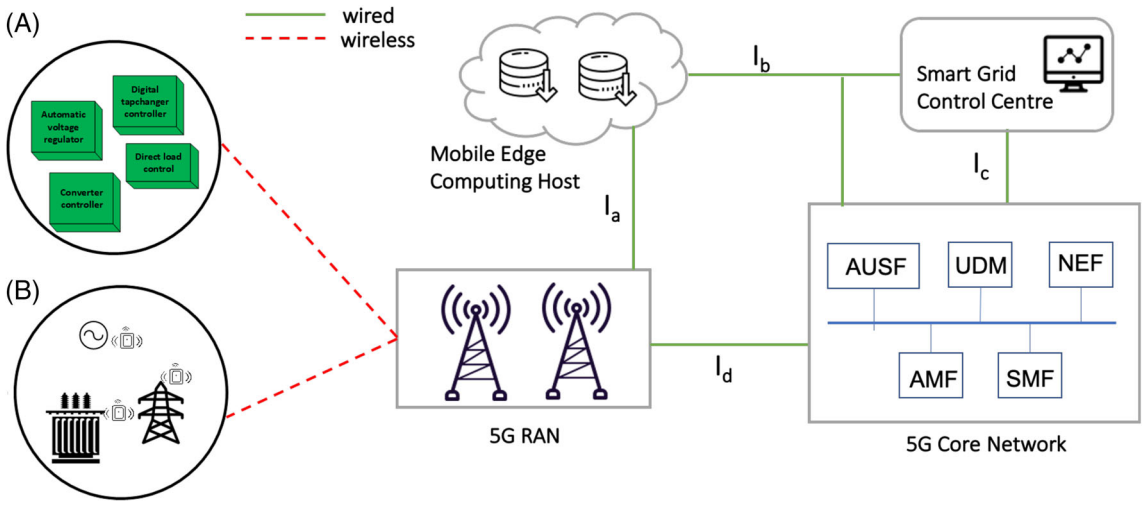

FIGURE 7 Enabling smart grid use case with 5G networks and IoT devices (type A and B)

use a gateway equipped with eSIM for reporting readings or measurement data to the SGCC. In addition, similar to work presented by Cherkaoui et al.,[62] 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[63] (e.g., security credentials or algorithms can be changed remotely over-the-air).

The eSIM or removable USIM in IoT devices or gateways contains 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 the corresponding IoT devices. The authentication is performed using Authentication and Key Agreement (AKA) or the EAP-AKA protocol.[61,64] 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[65]). However, there are a few privacy issues allowing tracking of 5G devices.[66] The smart grid operator can utilize the eSIM remote management framework to monitor or install add-on services (e.g., 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.[67] 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[61] (in our smart grid scenario, for example with DSO or an actor managing IoT device types A or B via the SGCC).

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,[61] 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, that is, end-to-end from IoT devices to the smart grid operation center. In this article, 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.[61] 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 purposes 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 protected, however, in 5G such traffic (e.g., feeder readings from Type A IoT devices) *is* integrity protected.[61] 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[68] or IPSec.[69]

Resiliency and availability: According to the FP7 FINESCE project,[33,70] 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.[33] also highlight a need of ultra-fast response requirement of a communication network for smart grids, specifically in the case of Phasor Measurement Units (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 DSOs require 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 the URLLC benefits of 5G network may be realized in 5G SA mode deployments, 5G security standardization (phase 2[71]) for URLLC services is being developed at the time of writing this article. Further, Wikström et al.[72] demonstrated how 5G URLLC can be used to provide line differential protection. Their research indicates that fiber based communications used between protection units[§] 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 stations specifically. The 5G security architecture supports legacy networks such as 4G, hence IoT based smart grids benefit from multi-network connectivity in terms of security and services when 5G radio is not available in some circumstances (e.g., 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 slices 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 the 5G core network enables the creation of network functions that can be scaled depending on the traffic load, or isolated under attack or network disruptions.

Role of Multi-Access Edge Computing Host (MECH): The real-time analysis of a large volume of data generated by IoT devices in smart grids requires the edge computing-based computational architecture. The 5G specifications offer edge computing enablers for data storage, processing, and hosting of applications close to the end-devices.[10] As shown in Figure 7, the node MECH plays the role of hosting third-party security and safety applications for our use case. The MECH allows the collection of huge amounts of data from IoT devices, and has processing capability to extract intelligent information before sending it to centralized servers. The extracted intelligent information enables the development of IoT or network threat detection applications using data analysis, Artificial Intelligence, and Machine Learning technologies. Many scenarios, for example,

[§]Malfunctions in the grid may lead to serious damage in the power grid infrastructure or to the connected consumer infrastructure (e.g., a factory or end-users). 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.[72]

monitoring of video frames for fire identification or identifying malicious control/data traffic from IoT devices, can be enabled via MECH. However, in public 5G networks, the DSO or TSO needs support from the mobile network provider to deploy smart grid specific MECH applications. In the case of private 5G networks, the MECH can be controlled by the DSO/TSO operator.

Security standard compliance: Compared to other non-cellular wireless technologies, 5G networks use 3GPP/ETSI standard compliant security protocols (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. Although this does not resolve security and trust issues in the IoT device supply chain and logistics, the network communication infrastructure may address such security issues in the upcoming 5G network due to dedicated 5G security certification and assurance related activities in the 3GPP.[73] For example, 5G network components such as base stations or dedicated hardware devices have to follow new 5G security certification and assurance schemes as specified by the 3GPP standard.

Non-public 5G networks: Compared with cellular networks offering services to general public users, a 5G non-public network (also referred to as private 5G networks) provides wireless network connectivity to a certain organization while deployed at their own premises; for example, a factory or corporate offices. Such type of non-public networks are ideal for enabling connectivity and automation for Industrial IoT (IIoT) devices, according to the 5G-ACIA group[¶]. 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, the 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.[74]

6 | 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 7, the 5G architecture is divided into the RAN and CN. The 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[#] are still possible against devices, including IoT. Shaik et al.[75] demonstrated that fake station type of attacks are possible in 5G, compromising privacy, denial of service and draining the battery of IoT devices. 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.
- Though 5G network provides the encryption and confidentiality protection for smart grid application data, the meta data may be exposed to the network provider. This metadata (radio signaling messages) includes device identities, connectivity points (e.g., server address), encrypted traffic patterns, and so forth. This may be relevant for AMI Infrastructure or battery charging stations. From the RAN perspective, fake base station attacks may compromise IoT device privacy, and downgrading attacks (by forcing fallback to 4G and 2G networks) may enable an attacker to steal data.
- The Next Generation Mobile Network (NGMN) group indicates potential security risks associated with the MECH node and related interfaces. Some examples are risks from user plane attacks, third party applications hosted in the MECH, and storage of security sensitive data at the edge node, as discussed by Zuo et al.[76] Hence, security misconfiguration issues at the MECH may affect the SGCC, or result in 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.[77] 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.
- Denial of service attacks against IoT devices over 5G may affect connectivity to IoT devices or sensors, potentially contributing to blackout scenarios in the smart grid. This is relevant considering the requirement of IoT devices to achieve self healing and automation concepts[78] in future smart grids.
- Threats associated with MECH, for example as outlined in the ENISA report.[79] This includes rogue gateway, overloading of the server, and abuse of edge open application programming interface by exploiting vulnerabilities in the applications running on multi edge computing type of applications.

[¶] 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.

[#] 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, a low-cost fake base station attack in 4G is demonstrated by Shaik et al.[65]

TABLE 2 Addressing threats with 5G

Security requirement	Threat (STRIDE)	5G contribution
Authentication	Spoofing	Fake base station prevention
		eSIM enables secure device authentication
Privacy	Information disclosure	eSIM key exchange enables encrypted communication
Availability	Denial of Service	5G split networks enhance resilience of individual base stations
		IoT network slices can be isolated from other slices
		5G supports fallback to legacy networks
Confidentiality	Information disclosure	eSIM key exchange enables encrypted communication
Integrity	Tampering	eSIM key exchange enables message authentication codes and authenticated encryption

7 | DISCUSSION

Automatic voltage control is mentioned as one of the main enabling technologies for distributed monitoring and control in active distribution networks.[14] Such applications will significantly increase the capacity of distribution networks for hosting increased numbers of DGs.[14] This is because the maximum amount of distributed generation that can be deployed on a given distribution feeder is often limited by the potential drop-off in voltage if the DER output suddenly drops off along the feeder.[80] In addition, realizing TSO-DSO reactive power management is mentioned as a major challenge for the future power system as reactive power resources connected to the transmission network are replaced by DERs (distributed generations, loads and storage elements) in the distribution network requiring more active operational coordination between TSOs and DSOs.[81] Hence, we selected the coordinated TSO-DSO reactive power management use case in this study, as it represents the most promising enabler in addition to it being a highly communication dependent application in the smart grid.

We have developed the voltage control scenario into a smart grid use case that highlights the requirements for secure communications. Further, we have studied and identified 5G security specification features and discussed their feasibility to meet security requirements for our IoT-enabled smart grid use case.

Using the STRIDE threat modeling approach, we have created a threat model of the smart grid use case that brings out important security challenges, some of which can be met by 5G. Table 2 gives an overview of how 5G contributes to meeting the posed security requirements and addressing the identified threats. By providing an overview of 5G security techniques that are applicable for the smart grid domain, we provide a foundation for future security analysis of 5G enabled smart grid systems.

We have no illusions that the introduction of 5G in the smart grid will solve all wireless security challenges, and we acknowledge that there are even potential new threats that are introduced from the 5G infrastructure itself. However, looking back on decades of computer security history, we realize that the only successful path is that of continual improvement. Recent experience from Ukraine[82] has shown us that the threat posed by external attackers is real, and complacency is the path to perdition.

For further work, we would like to perform a laboratory implementation of our use case which would allow us to implement specific misuse cases[49] to validate identification and mitigation methods, as part of a broader study of controller architecture and resilience. Furthermore, though we have presented a threat model for our use case, a natural next step is to develop a threat model for the entire smart grid ecosystem.

8 | CONCLUSION

The use of IoT devices promises digital transformation to several domains, including the current power grid infrastructure. However, IoT security is still challenging in a smart grid infrastructure, partly considering tradeoffs between cost and performance. In this article, we have identified IoT communication requirements in a low-voltage regulation smart grid use case and developed an associated threat model. We have studied 5G specifications and discussed their security application on the selected smart grid use case. Although 5G networks do not solve all IoT security problems, they do provide an alternative reliable communication channel with built-in security benefits for the smart grid infrastructure.

In terms of implications for science, this article have summarized the state of the art for smart grid security when using 5G for IoT networking. We have documented a specific use case that can be used for assessing future security mechanisms. We have identified several areas of further work, not least the need to perform laboratory studies on deployment-scale 5G IoT networks. For practitioners, we have presented a threat model for our limited use case which can be employed by DSOs who are in the process of updating their substation communication strategies. We have provided information on what 5G can offer DSOs in terms for security aspects, and on what limitations remain to be considered.

ACKNOWLEDGMENTS

This work is funded by CINELDI—Centre for intelligent electricity distribution, an 8-year Research Centre under the FME-scheme (Centre for Environment-friendly Energy Research, 257626/E20) and Raksha: 5G Security for Critical Communications (312122), a four-year project funded under the IKTPLUSS-IKT og Digital Innovasjon programme. The authors gratefully acknowledge the financial support from the Research Council of Norway and the CINELDI partners. https://www.sintef.no/cineldi/

ORCID

Ravishankar Borgaonkar https://orcid.org/0000-0003-2874-3650
Inger Anne Tøndel https://orcid.org/0000-0001-7599-0342
Merkebu Zenebe Degefa https://orcid.org/0000-0002-8576-3693
Martin Gilje Jaatun https://orcid.org/0000-0001-7127-6694

REFERENCES

1. Line MB, Tøndel IA, Jaatun MG. Cyber security challenges in Smart Grids, 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies. Manchester, UK; 2011:1-8. https://doi.org/10.1109/ISGTEurope.2011.6162695
2. ENISA Baseline security recommendations for IoT in the context of critical information infrastructures. ENISA report; 2017. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.
3. Borgaonkar R, Jaatun MG. 5G as an Enabler for Secure IoT in the Smart Grid: Invited Paper, 2019 First International Conference on Societal Automation (SA). Krakow, Poland; September 4-6, 2019:1-7, IEEE. https://doi.org/10.1109/SA47457.2019.8938064.
4. Islam SN, Baig Z, Zeadally S. Physical layer security for the smart grid: vulnerabilities, threats, and countermeasures. *IEEE Trans Ind Inform*. 2019;15(12):6522-6530.
5. European Union 5G deployment could bring millions of jobs and billions of euros benefits, study finds. DG CONNECT; 2016.
6. NRG5 Project- enabling smart energy as service via 5G network advances; 2019. http://www.nrg5.eu.
7. WIVE Project- wireless for verticals; 2019. https://wive.turkuamk.fi.
8. SOGNO Project- service oriented grid for the network of the future; 2019. https://www.sogno-energy.eu.
9. 3GPP New WID on 5G smart energy and infrastructure. meeting document; 2020. https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_88E_Electronic/Docs/SP-200574.zip.
10. Kekki S, Featherstone W, Fang Y, et al. MEC in 5G networks; 2018. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_m%ec_in_5G_FINAL.pdf.
11. Cosovic M, Tsitsimelis A, Vukobratovic D, Matamoros J, Anton-Haro C. 5G mobile cellular networks: enabling distributed state estimation for smart grids. *IEEE Commun Mag*. 2017;55(10):62-69.
12. Zerihun TA, Garau M, Helvik BE. Effect of communication failures on state estimation of 5G-enabled smart grid. *IEEE Access*. 2020;8:112642-112658.
13. Eurelectric, power distribution in Europe – facts & figures; 2013. https://www3.eurelectric.org/powerdistributionineurope/d/2013/12.105/46.
14. D'Adamo C, Abbey C, Baitch A, et al., Development and operation of active distribution networks, CIGRÉ; 2011.
15. SMB Smart Grid Strategic Group (SG3), IEC smart grid standardization roadmap; 2010. http://www.itrco.jp/libraries/IEC-SmartgridStandardizationRoadmap.pdf
16. Fang X, Misra S, Xue G, Yang D. Smart grid – the new and improved power grid: a survey. *IEEE Commun Surv Tutor*. 2012;14(4):944-980.
17. Ericsson GN. Cyber security and power system communication–essential parts of a smart grid infrastructure. *IEEE Trans Power Deliv*. 2010;25(3):1501-1507.
18. Zunino C, Valenzano A, Obermaisser R, Petersen S. Factory communications at the dawn of the fourth industrial revolution. *Comput Stand Interf*. 2020;71:103433. https://www.sciencedirect.com/science/article/pii/S0920548919300868
19. The 5G economy: how 5G will impact global industries, the economy, and you; 2019. https://www.technologyreview.com/s/603770/the-5g-economy-how-5g-will-impact-global-industries-the-economy-and-you/.
20. Pliatsios D, Sarigiannidis P, Goudos S, Karagiannidis GK. Realizing 5G vision through cloud RAN: technologies, challenges, and trends. *EURASIP J Wirel Commun Netw*. 2018;2018(1):136. https://doi.org/10.1186/s13638-018-1142-1
21. 5G Implementation Guidelines; 2019. https://www.gsma.com/futurenetworks/wp-content/uploads/2019/03/5G-Implementation-Guideline-v2.0-July-2019.pdf.
22. Non-standalone and Standalone: two standards-based paths to 5G; 2019. https://www.ericsson.com/en/blog/2019/7/standalone-and-non-standalone-5g-nr-two-5g-tracks.
23. Yun M, Yuxin B. Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, 2010 International Conference on Advances in Energy Engineering. Beijing, China; 2010:69-72. https://doi.org/10.1109/ICAEE.2010.5557611.
24. Ou Q, Zhen Y, Li X, Zhang Y, Zeng L. Application of Internet of Things in Smart Grid Power Transmission, in 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC). Vancouver, BC; 2012:96-100. https://doi.org/10.1109/MUSIC.2012.24.
25. Liu J, Li X, Chen X, Zhen Y, Zeng L. Applications of Internet of Things on smart grid in China, 13th International Conference on Advanced Communication Technology (ICACT2011). Gangwon, Korea (South); 2011:13-17.
26. Saleem Y, Crespi N, Rehmani MH, Copeland R. Internet of Things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions. *IEEE Access*. 2019;7:62962-63003. https://doi.org/10.1109/ACCESS.2019.2913984
27. Frustaci M, Pace P, Aloi G, Fortino G. Evaluating critical security issues of the IoT world: present and future challenges. *IEEE Internet Things J*. 2018;5(4):2483-2495.
28. Carlsson A. *On the Use of 5G for Smart Grid Inter-Substation Control Signaling* [MSc thesis]. Karslstad University; ; 2019.

29. Garau M, Anedda M, Desogus C, Ghiani E, Murroni M, Celli G. A 5G cellular technology for distributed monitoring and control in smart grid, 2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB). Cagliari, Italy; 2017:1-6. https://doi.org/10.1109/BMSB.2017.7986141.
30. Nguyen V, Grinnemo K, Taheri J, Brunstrom A. A Deployable Containerized 5G Core Solution for Time Critical Communication in Smart Grid, 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN). Paris, France; 2020:153-155. https://doi.org/10.1109/ICIN48450.2020.9059397.
31. SliceNet EU Project - 5G smart grid self-healing use case; 2020. https://slicenet.eu/5g-smart-grid-self-healing-use-case/.
32. Moongilan D. 5G wireless communications (60 GHz band) for smart grid – An EMC perspective, 2016 IEEE International Symposium on Electromagnetic Compatibility (EMC). Ottawa, Canada; 2016:689-694. https://doi.org/10.1109/ISEMC.2016.7571732.
33. Leligou HC, Zahariadis T, Sarakis L, Tsampasis E, Voulkidis A, Velivassaki TE. Smart Grid: a demanding use case for 5G technologies. Paper presented at: Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops); 2018.
34. Saghezchi FB, Mantas G, Ribeiro J, Al-Rawi M, Mumtaz S, Rodriguez J. Towards a secure network architecture for smart grids in 5G era, 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC). Valencia, Spain; 2017:121-126. https://doi.org/10.1109/IWCMC.2017.7986273.
35. El Mrabet Z, Kaabouch N, El Ghazi H, El Ghazi H. Cyber-security in smart grid: Survey and challenges. *Comput & Electr Eng*. 2018;67:469-482. https://doi.org/10.1016/j.compeleceng.2018.01.015. https://www.sciencedirect.com/science/article/pii/S0045790617313423.
36. Gunduz MZ, Das R. Cyber-security on smart grid: threats and potential solutions. *Comput Netw*. 2020;169:107094.
37. Pliatsios D, Sarigiannidis P, Lagkas T, Sarigiannidis AG. A survey on SCADA systems: secure protocols, incidents, threats and tactics. *IEEE Commun Surv Tutor*. 2020;22(3):1942-1976.
38. De Dutta S, Prasad R. Security for smart grid in 5G and beyond networks. *Wirel Pers Commun*. 2019 May;106(1):261-273. https://doi.org/10.1007/s11277-019-06274-5
39. Kimani K, Oduol V, Langat K. Cyber security challenges for IoT-based smart grid networks. *Int J Critical Infrastruct Protect*. 2019;25:36-49. http://www.sciencedirect.com/science/article/pii/S18745482173%01622
40. Bekara C. Security issues and challenges for the IoT-based smart grid. *Proc Comput Sci*. 2014;34:532-537. http://www.sciencedirect.com/science/article/pii/S1877050914009193 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.
41. Khavari A, Montoya J, Graditi G, et al. INTERPLAN use cases. deliverable D3 2 INTERPLAN project; 2018.
42. Gungor VC, Sahin D, Kocak T, et al. A survey on smart grid potential applications and communication requirements. *IEEE Trans Ind Inform*. 2012;9(1):28-42.
43. Daratha N, Das B, Sharma J. Coordination between OLTC and SVC for voltage regulation in unbalanced distribution system distributed generation. *IEEE Trans Power Syst*. 2013;29(1):289-299.
44. Shahid K, Kidmose E, Olsen RL, Petersen L, Iov F. On the impact of cyberattacks on voltage control coordination by ReGen plants in smart grids. Paper presented at: Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm); 2017:480-485.
45. Hug G, Giampapa JA. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *IEEE Trans Smart Grid*. 2012;3(3):1362-1370. https://ieeexplore.ieee.org/document/6275516.
46. Onogawa M, Yoshizawa S, Fujimoto Y, et al. Enhancing security for voltage control of distribution systems under data falsification attacks. Paper presented at: Proceedings of the 2019 American Control Conference (ACC); 2019:3249-3254.
47. Wang W, Lu Z. Cyber security in the smart grid: survey and challenges. *Comput Netw*. 2013;57(5):1344-1371. https://dl.acm.org/doi/10.5555/2459506.2459606.
48. Liu J, Xiao Y, Li S, Liang W, Chen CP. Cyber security and privacy issues in smart grids. *IEEE Commun Surv Tutor*. 2012;14(4):981-997.
49. Tøndel IA, Borgaonkar R, Jaatun MG, Frøystad C. What could possibly go wrong? smart grid misuse case scenarios. Paper presented at: Proceedings of the 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security); 2020:1-8.
50. Otuoze AO, Mustafa MW, Larik RM. Smart grids security challenges: classification by sources of threats. *J Electr Syst Inf Technol*. 2018;5(3):468-483. https://doi.org/10.1016/j.jesit.2018.01.001.
51. Pillitteri VY, Brewer TL. *Guidelines for Smart Grid Cybersecurity*. Gaithersburg, MD: NIST; 2014. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.
52. ETSI Study of use cases and communications involving IoT devices in provision of emergency situations. (ETSI); 2019.
53. Goldreich O. *Foundations of Cryptography: Volume 2, Basic Applications*. New York, NY: Cambridge University Press; 2004.
54. Falliere N, Murchu LO, Chien E, W32.Stuxnet Dossier; 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
55. Cherepanov A, Lipovsky R, Industroyer: Biggest threat to industrial control systems since Stuxnet. WeLiveSecurity by eset; 2017. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-\LY1\textbackslash-stuxnet/.
56. Kovacs E. New εTritonε ICS malware used in critical infrastructure attack. SecurityWeek; 2017. https://www.securityweek.com/new-ics-malware-triton-used-critical-infrastructure-attack.
57. Watts R, Kline B, Ridge T, Potential electric grid vulnerability from cyber enabled foreign actors. protect our power; 2018. https://protectourpower.org/wp-content/uploads/2018/11/Ridge-Global-and-Potential-Electric-Grid-Vulnerability.pdf.
58. Tøndel IA, Jaatun MG, Line MB. Threat Modeling of AMI. In: Hämmerli BM, Kalstad Svendsen N, Lopez J, eds. Critical Information Infrastructures Security. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg; 7722. https://doi.org/10.1007/978-3-642-41485-5_23.
59. Shostack A. Experiences threat modeling at Microsoft. Paper presented at: Proceedings of the Modeling Security Workshop; 2008. http://blogs.msdn.com/cfs-file.ashx/__key/communityserver-components-postattachments/00-08-99-18-06/Shostack_2D00_ModSec08_2D00_Experiences_2D00_Threat_2D00_Modeling_2D00_At_2D00_Microsoft.pdf, http://www.comp.lancs.ac.uk/modsec/program.php.
60. Swiderski F, Snyder W. *Threat Modeling*. Redmond, WA: Microsoft Press; 2004. https://dl.acm.org/doi/10.5555/983226.
61. Technical Specification 33.501, Security architecture and procedures for 5G System. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169.
62. Cherkaoui A, Bossuet L, Seitz L, Selander G, Borgaonkar R. New paradigms for access control in constrained environments. Paper presented at: Proceedings of the 2014 9th International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC); 2014:1-4.

63. SIMalliance, SIMs, eSIMs and secure elements. 5G security; 2019. https://docbox.etsi.org/Workshop/2019/201906_ETSISECURITYWEEK/202106_DynamicNatureOfTechno/SESSION02_IoTDEVICESandSERVICES/SIMalliance_CRICCO.pdf.
64. Arkko J, Lehtovirta V, Eronen P, Improved extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA'). IETF. RFC 5448 (Informational); 2009. http://www.ietf.org/rfc/rfc5448.txt.
65. Shaik A, Seifert J, Borgaonkar R, Asokan N, Niemi V. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. Paper presented at: Proceedings of the 23rd Annual Network and Distributed System Security Symposium, NDSS 2016; February 21-24, 2016; San Diego, CA.
66. Borgaonkar R, Hirschi L, Park S, Shaik A. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. Paper presented at: Proceedings of the 19th Privacy Enhancing Technologies Symposium, PETS 2019; 2019.
67. Norrman K, Nakarmi PK, Fogelström E, 5G Security; 2019. https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system.
68. Rescorla E. The transport layer security (TLS) protocol version 1.3. RFC Editor. RFC 8446; 2018. https://rfc-editor.org/rfc/rfc8446.txt.
69. Seo K, Kent S. Security architecture for the internet protocol. RFC Editor. RFC 4301; 2005. https://rfc-editor.org/rfc/rfc4301.txt.
70. FINESEC Project- integrated framework for predictive and collaborative security of financial infrastructures; 2019. https://www.finsec-project.eu/.
71. Prasad AR, Zugenmaier A, Escott A, Soveri MC. 3GPP 5G security; 2018. https://www.3gpp.org/news-events/1975-sec_5g.
72. Wikström G, Torsner J, Kronander J, et al. Wireless protection of power grids over a 5G network. Paper presented at: Proceedings of the 2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia); 2019:976-981.
73. 3GPP Security assurance specification (SCAS) for the next generation Node B (gNodeB) network product class. (3GPP); 2019.
74. 5G-ACIA group whitepaper, 5G non-public networks for industrial scenarios; 2019. https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-AC%IA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios/5G-ACIA_Whi%te_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios.pdf.
75. Shaik A, Borgaonkar R, Park S, Seifert JP. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. Paper presented at: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks WiSec '19; 2019:221-231; ACM, New York, NY. https://doi.org/10.1145/3317549.3319728.
76. NGMN Alliance 5G security Package 3: mobile edge computing / low latency / consistent user experience. NGMN; 2018.
77. Zuo M, Wang K, Zhuang X, et al. Security aspects of network capabilities exposure in 5G. NGMN alliance; 2018.
78. Elgenedy MA, Massoud AM, Ahmed S. Smart grid self-healing: functions, applications, and developments. Paper presented at: Proceedings of the 2015 1st Workshop on Smart Grid and Renewable Energy (SGRE); 2015:1-6.
79. ENISA Threat landscape for 5G networks. ENISA report; 2019. https://www.enisa.europa.eu/publications/enisa-threat-landsca%pe-for-5g-networks/at_download/fullReport.
80. Madrigal M, Uluski R, Gaba KM. *Practical Guidance for Defining a Smart Grid Modernization Strategy: The Case of Distribution (Revised Edition)*. Washington, DC: World Bank Publications; 2017. https://openknowledge.worldbank.org/handle/10986/26256.
81. Sun H, Guo Q, Qi J, et al. Review of challenges and research opportunities for voltage control in smart grids. *IEEE Trans Power Syst*. 2019;34(4):2790-2801.
82. Lee RM, Assante MJ, Conway T, Analysis of the cyber attack on the Ukrainian power grid, defense use case. SANS ICS and E-ISAC white paper; 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

How to cite this article: Borgaonkar R, Anne Tøndel I, Zenebe Degefa M, Gilje Jaatun M. Improving smart grid security through 5G enabled IoT and edge computing. *Concurrency Computat Pract Exper*. 2021;e6466. https://doi.org/10.1002/cpe.6466