Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5G-Enabled Smart City Infrastructure for Critical Power and Utility Management

[1]Malik Husnain Abbas*, [2]Ashish Waghre, [3]Sajid Khot, [4]Salman Khan
1. Electrical Design Riyadh Metro Transit, SYSTRA Riyadh Sa, Riyadh, Saudi Arabia
2. IT-District Technology Management, KAFD Development & Management Company, Riyadh, Saudi Arabia
3. IT-District Technology Management, KAFD Development & Management Company, Riyadh, Saudi Arabia
4. Application Operations, Siemens - Saudi Telecom Company (STC), Riyadh, Saudi Arabia
**Corresponding Author: engr.ham@gmail.com*

ARTICLE INFO

Received: 24 Oct 2024

Revised: 12 Nov 2024

Accepted: 26 Dec 2024

ABSTRACT

The high rate of the development of the fifth-generation (5G) wireless network offers the revolutionary possibilities of the smart city implementation, especially in the critical power and utility management systems. This essay explores the architectures, communication schemes and implementation plans related to 5G-enabling smart city infrastructure with a particular focus on electricity grids, water distribution systems, and gas utility networks. Our analysis covers the main 5G characteristics ultra-reliable low-latency communication (URLLC), massive machine-type communication (mMTC), and enhanced mobile broadband (eMBB), and how they can be used to the monitoring of real-time, fault detection, demand response, and grid automation. An analysis between the current communication paradigms (4G LTE, ZigBee, LoRaWAN, and WiSUN) and 5G is done based on latency, bandwidth, scalability, and reliability. The security issues, such as spoofing, jamming, and man-in-the-middle attacks, are addressed, as well as mitigation solutions that utilize network slicing, edge computing, and blockchain-based access control. To confirm theoretical propositions, case studies of pilot deployments in South Korea, the UAE, and India are included. The results prove that 5G has a great positive impact on utility operational efficiency up to 40 percent, decrease of outage detection time to less than 10 milliseconds and facilitating the seamless integration of distributed energy resources (DERs). The article adds the perspective of a holistic approach to the synergistic relationship between 5G connectivity and smart utility management to provide a guideline when adopting large scale deployments in the city in the future.

Keywords: 5G networks, smart city, critical infrastructure, power grid, utility management, URLLC, mMTC, network slicing, edge computing, IoT.

I. INTRODUCTION

Smart cities are becoming more dependent on a networked digital infrastructure to streamline the operations of cities, their resources and public services. Power and utility management systems are some of the most important elements of any modern smart city that include electricity grids, water supply networks, and gas distribution pipelines. The qualities of resilience, efficiency, and intelligence of such systems are directly related to the quality of underpinning communication infrastructure [1]. Early smart grid implementations have been on the backbone of traditional communication technologies like power line communication (PLC), ZigBee and legacy cellular networks. Nonetheless, the technologies have inherent constraints of latencies, throughput and scalability which are increasingly disrupting real time needs of contemporary smart utility operations [2]. With the expansion of urban population and energy requirements going more dynamic due to the inclusion of renewable energy, the use of electric vehicles (EV) and decentralized prosumer model, the need to shift towards a new paradigm in communication infrastructure emerges [3].

The 3rd Generation Partnership Project (3GPP) standardized 5G wireless technology under Release 15 and later releases, proposes three fundamental categories of service that can be of tremendous value to smart utility applications [4]. Enhanced Mobile Broadband (eMBB) proposes high throughput-connected solutions with infrastructure inspection based on videos and augmented reality maintenance. The Ultra-Reliable Low-Latency Communication (URLLC) provides grid automation in real-time and with end-to-end latencies that are less than a millisecond. Massive Machine-Type Communication (mMTC) helps millions of low-power smart meters and sensor nodes to be connected at the same time [5].

Although non-standardised treatment of an integration of 5G into all the utility domains power, water and gas has been the focus of considerable academic and industrial scrutiny and interest, there has been little detailed coverage of such a system both architecturally and operationally in the literature. This gap is filled in this paper which offers a systematic study of 5G-enabled infrastructure of a smart city in the forms of communication architecture, challenges of deploying smart cities, security factor, and empirical performance results. This work made the following contributions:

- Systematic analysis of the 5G architectural elements and how they are mapped to the needs of smart utility communications.
- Comparison of 5G with existing communication technologies in useful applications.
- A 5G-based critical infrastructure-specific taxonomy and mitigation framework of security threats.
- A practical test which is done by using real-world pilot deployments in three different geographies.
- Design considerations and future research problems on possible 5G smart city applications.

The rest of this paper is structured according to the following way: Section II is related work, Section III is 5G system architecture of smart utilities, Section IV is the analysis of key enabling technologies, Section V is the comparison of 5G and the current communication paradigms, readings, Section VII are the deployment case studies and Section VII is the conclusion and future research directions.

II. RELATED WORK

The convergence of cellular communication and smart grid have been widely discussed in scholarly literature since the first rollouts of Advanced Metering Infrastructure (AMI) on 3G/4G LTE networks. Gungor et al. [6] suggested a pioneer taxonomy of communication technologies in smart grids, differentiating between wired and wireless systems, and bandwidth-latency trade-offs as one of the key design considerations. Their work developed the vocabulary that is in use in 5G-smart grid literature.

Agiwal et al. [7] anticipated the shift towards 5G utility applications by surveying the development of 4G LTE-Advanced into 5G considering the heterogeneous network architecture, beamforming, and massive MIMO. This set of properties was later investigated with respect to smart grid communication by Hossain et al. [8] which established that millimeter-wave (mmWave) 5G channels had potential to meet substation automation standards outlined in the IEC 61850 standard, such as GOOSE messages and latency requirements of less than 4 milliseconds.

The concept of network slicing became important in the study of utility communication after initial work done by Foukas et al. [9] who postulated a slicing framework that allows logical network segregation of various utility areas. Expanding on this, Liang et al. [10] came up with a model of optimizing the resource allocation in 5G network slicing within smart grid applications and showed that they could bring about significant changes in quality of service (QoS) of the heterogeneous utility traffic. In their model, they found that fault isolation time inherent to communication could be reduced by 67% in dedicated URLLC slices as opposed to when communicating in a shared network space.

Mao et al. [11] investigated the concept of Mobile Edge Computing (MEC) integration with smarter grids and showed that offloading the task of smart meter devices to the server at their edges can reduce the amount of computational latency time up to hundreds of milliseconds to almost real-time. This was in line with the bigger edge-AI model that Zhou et al. [12] discussed, where federated learning is applied at the network edge to facilitate privacy-guaranteed demand prediction in distributed energy sources.

Ahmad et al. [13] have enumerated attack vectors such as rogue base stations, signaling storms, and protocol-level exploits (in 5G Non-Standalone (NSA) and Standalone (SA) architectures) and provided guidelines on mitigating security vulnerabilities that are particular to 5G utility infrastructure. In line with this, Ferrag et al. [14] suggested a blockchain authentication scheme of 5G-IoT devices in critical infrastructure and showed it to be resistant to Sybil attacks as well as replay attacks in a simulated environment.

Although these contributions discuss the individual points of 5G-based utility communication, none of them makes an integrated analysis of architecture and empirical analysis across the areas of power, water, and gas utility. This paper generalizes these previous works and also elaborates them through cross-domain architectural modelling and analysis of multi-geography cases study.

III. 5G SYSTEM ARCHITECTURE FOR SMART UTILITY MANAGEMENT

A. 5G Network Architecture Overview

Architectural 5G System According to 3GPP Release 16 and 17, the architecture is divided into three functionality planes, which are the radio access network (RAN), the 5G core (5GC) and the application layer [15]. RAN is made up of Next-Generation NodeB (gNB) base stations which are interconnected through Xn interface. A 5G core is service-based (just as the 4G LTE evolved packet core, are), based on microservices, instead of the monolithic evolved packet core (EPC). The most important 5GC functions are the: Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF), and the Network Exposure Function (NEF) [4].

In the case of smart utility, the UPF location in the network edge is of critical importance. Local UPF breakout allows data paths of ultra-low latency between field devices and utility control systems to occur, bypassing latency penalties of centralized routing in a data center. This deployment topology is in agreement with Multi-Access Edge Computing (MEC) that is a standard of ETSI [16].

B. Isolation of utility Traffic on Slices.

Network slicing allows the creation of a variety of logically separated virtual networks on a common physical 5G infrastructure. In the case of utility management, there are three main types of slices that are distinguished [9], [10]:

- URLLC Slice: For protection relay communication, fault isolation as well as SCADA control commands, with end-to-end latency requirement of less than 5 ms and packet error rate (PER) requirement of less than 105.
- mMTC Slice: Enabling support of data collection of mass smart meters, pressure sensors, IoT endpoints with densities of connections up to 106 devices/km2.
- eMBB Slice: Enabling high-definition video surveillance of substations, AR/VR-enhanced applications to support technicians during infrastructure inspection via drones, and supporting technician training.

The isolation of slices is provided by special Radio Access Network (RAN) resources which are assigned using network slice selection assistance information (NSSAI) signaling. The isolation of core networks is obtained through the independent amounts of UPF and through the different names of data network (DNNs) per slice [15].

C. Edge Computing Integration.

Integration of MEC servers in gNB sites or aggregation stations forms a distributed computing layer, which can support utility analytics applications, near field devices. This architecture minimizes round trip latency of time sensitive processes like voltage regulation, protection coordination and demand response dispatch. Applications hosted on MEC are real time state estimation engines, AI based anomaly detection algorithms and digital twin synchronization services [11].

The URLLC utility traffic communication route is as follows: Field Device → gNB → Local UPF → MEC Server → Local Control Application and is optional but may have a backhaul to the central Utility Management System (UMS) over the 5GC. This architecture is able to provide control plane operations latencies of 2-8 ms end-to-end, which is significantly less than the IEC 61850 requirement of 2 ms to be used in protection applications [17].

IV. KEY ENABLING TECHNOLOGIES

A. Ref. Massive MIMO and Beamforming.

Massive Multiple-Input Multiple-Output (Massive MIMO) uses 64-256 elements of antenna arrays at gNB sites to form spatially targeted beams greatly enhancing spectral efficiency and network capacity [7]. Massive MIMO has been proven to give good signal penetration in metallic enclosures as well as industrial interference environments in utility environments especially outdoor substations and pipeline corridors. Beamforming can also minimize inter-device interference in dense networks of smart meters, which can support the density of mMTC communication needed by applications of AMI.

B. mmWave Communication B. Millimeter Wave (mmWave).

Multi-gigabit per second throughput is achievable with 5G mmWave (24100 GHz) that has channel bandwidths of 400 MHz or higher [7]. Although the mmWave propagation nature gives them a range of 100-300m and can be easily blocked, they are ideal intra-substation communication networks, industrial campus networks, and point-to-point links backhaul between utility relay stations. The large bandwidth provides the possibility to transmit both high-frequency data streams of power quality (1 kHz PMU sampling rates) and video surveillance streams [8].

C. Device-to-Device (D2D) and Sidelink Communication.

A sidelink communication allows the direct device to device communication without going through the base station and offers a robust method to communicate during falls as a backup data transmission system in the event that network infrastructure has been destroyed by power or natural disasters [5]. As a smart city utility management, D2D sidelink can be used to allow peer-to-peer utilities among smart meters under backhaul failures to keep a local demand data aggregation in place, as well as mesh-based fault reporting.

D. Time-Sensitive Networking (TSN) Integration.

Implementing 5G in conjunction with IEEE 802.1 Time-Sensitive Networking (TSN) standards allows delivering packets in a deterministic manner with a limited latency and zero losses due to congestion, which are important in industrial automation systems in the utility substation [18]. In 3GPP Release 16, standard architecture 5G-TSN bridge is used to convert TSN timing information across the 5G air interface to allow protection relays, merging units and phasor measurement units (PMUs) in geographically separated substations to operate synchronized.

E. Edge-based AI and ML.

MEC servers are used to deploy edge AI capabilities to process utility telemetry streams in real-time without the need to connect to the cloud. Convolutional neural networks (CNNs) and long short-term memory (LSTMs) models have also been shown to work in non-intrusive load monitoring (NILM), prediction of faults in transformers based on dissolved gas analysis such as dissolved gas analysis (DGA), and detection of leaks in water networks using pressure transient signals [12]. Federated learning systems allow model training in a state of distributed smart meters without personal consumption information being exchanged with the central servers and can mitigate privacy requirements [14].

V. COMPARATIVE ANALYSIS OF COMMUNICATION TECHNOLOGIES.

Comprehensive comparative analysis of 5G and existing utility communication technologies used by infrastructure is required in the planning, and investment decision making. The comparison of latency, data rate, range, device density, reliability and general utility appropriateness has been multi-dimensionally compared in the table I.

TABLE I: Comparative Analysis of Communication Technologies for Smart Utility Management

Technology	Latency	Data Rate	Range	Device Density	Reliability	Utility Suitability
5G NR (URLLC)	< 1 ms	Up to 20 Gbps	< 500 m (mmWave)	10^6/km²	99.9999%	Excellent

Technology	**Latency**	**Data Rate**	**Range**	**Device Density**	**Reliability**	**Utility Suitability**
4G LTE	10–50 ms	100–150 Mbps	1–5 km	10^5/km^2	99.99%	Good
LoRaWAN	1–10 s	250–5400 bps	2–15 km	10^4/km^2	99%	Limited
ZigBee (IEEE 802.15.4)	5–20 ms	250 kbps	10–100 m	10^3/km^2	99.9%	Limited
Wi-SUN	50–100 ms	300 kbps	1–3 km	10^4/km^2	99.5%	Moderate
PLC (Narrowband)	100–500 ms	1–500 kbps	1–10 km	10^3/km^2	97%	Poor

Table I shows that 5G URLLC has a lower latency performance by a factor of 10 or more than 4G LTE and many orders of magnitude lower than the LPWAN 5G - LoRaWAN technology. This protection relay performance benefit is essential when used in applications requiring protection of grids with operating time delays due to communication that exceed 5 ms [8].

Although LoRaWAN and Wi-SUN have better range capabilities, which would be useful in the rural utility corridor monitoring, their throughput and latency limit prohibits adopting it in closed-loop control in deployment. The hybrid system architecture connecting both the control-plane communication app and protection with 5G URLLC, and non-time-critical AMI data collection with the LPWAN is the most suitable as a technoeconomic implementation strategy of smart city utility networks [6].

The 5G mMTC device density advantage (up to 10 6 devices/km 2) is also notable when it comes to densely populated cities smart meters systems. Smart City implementations in Seoul and Dubai have been analyzed, which confirmed that the high communication traffic of metering by top-of-hour intervals exceeds 4G LTE capacity limits at grid segments of central business districts that have a meter density of over 2,000 per km2 [19].

VI. MITIGATION STRATEGIES AND SECURITY CHALLENGES.

A. Threat Taxonomy of 5G utility networks.

Both state-sponsored and financially driven threat agents are valuable targets of critical infrastructure communication networks. Ahmad et al. [13] include in 5G-particular attack vectors 3 threat levels: physical layer (jamming, pilot contamination), protocol layer (signaling exploitation, slice isolation breach), and application layer (SCADA protocol injection, false data bidding in AMI networks). The spread of IoT endpoints used in the smart utility implementation grows exponentially in attack surface over conventional operation technology (OT) applications.

An especially advanced type of threat to the infrastructure of smart meters can be false data injection (FDI), which allows attackers to poison state estimation functions with the energy management system (EMS) without being detected by traditional bad data-detecting methods [20]. In water distribution networks, integrity attacks can involve pressure sensor readings in order to cover up impending failures in the pipes, or to permit contamination incidents.

B. Mitigation Framework

The suggested security architecture is a layered one, which includes the following mechanisms [13], [14]:

- Network Slicing Isolation The isolation of slice-to-slice movements in 5G Security Anchor Functions (SEAF) via the use of cryptography ensures that application slices cannot vertically or horizontally migrate with each other. URLLC protection slices are not shared with eMBB surveillance slices and in case of compromise, blast radius is restricted.

- IoT device authentication with blockchain: With millions of IoT devices on smart utilities networks, distributed ledger technology ensures an immutable identity management system to oversee an endpoint. Smart contracts are access control policies that implement least-privilege policies against communication without central authentication infrastructure single points of failure.
- AI-based Anomaly Detection: The deep learning-based models deployed on MEC servers collectively monitor behavior of device communications in real-time and determine compromised devices that are associated with anomalous reporting rates, data values, or communication destinations.
- Physical Layer Security: Massive MIMO beamforming offers physical layer security with spatial multiplexing in massively MIMO system; passive eavesdropping is much more challenging than with omnidirectional legacy systems.
- Zero-Trust Architecture Zero-trust is used to guarantee per-session authorization of all communication between teams in the 5G utility communication network by making the network perimeter boundaries have zero trust and ensure that implicit trust exists there.

C. Regulatory and Standards Compliance.

The deployments of critical infrastructure based on 5G need to meet the requirements of relevant cybersecurity guidelines such as NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) standards, the power systems communication safety requirements of IEC 62351, and the NIST Cybersecurity Framework. The 5G security architecture as delineated in 3GPP TS 33.501, offers basic security features such as 256-bit encryption, integrity protection, and subscriber identity concealment through SUCI in line with such regulatory priorities [15].

VII. REAL-WORLD CASE STUDIES OF DEPLOYMENT.

Potential outcomes are tested by three pilot deployments to add credence to the theoretical constructions introduced in the previous sections. This Table II is a summary of major deployment parameters and performance results of the three case study locations.

TABLE II: Summary of 5G Smart Utility Pilot Deployment Outcomes

Parameter	**Seoul, South Korea**	**Dubai, UAE**	**Bengaluru, India**
Deployment Year	2021	2022	2023
Utility Domain	Electricity Grid	Water + Power	Multi-utility
5G Architecture	SA (Release 16)	NSA → SA Migration	NSA (Release 15)
Connected Devices	1.2 million	850,000	320,000
Avg. Latency	3.2 ms	5.1 ms	8.7 ms
Fault Detect. Time	< 8 ms	< 12 ms	< 18 ms
Efficiency Gain	42%	38%	31%
Network Slices	4 (URLLC+mMTC+eMBB +Mgmt)	3 (URLLC+mMTC+eMBB)	2 (URLLC+mMTC)

A. Seoul Metropolitan Smart Grid (South Korea)

The Seoul Smart Grid Initiative was a project of Samsung Networks together with Korea Electric Power Corporation (KEPCO) to install a 5G Standalone network with 1.2 million smart meters and 3,400 distribution substations in Seoul metropolitan area [21]. The installation relies on special URLLC network slices on protection relay interstation communication between distribution substations with measured end-to-end latency of 3.2 ms - much lower than IEC 61850 GOOSE message specifications. Demand Response, which operated via the 5G platform met a cost of 42 percent lower than the previous system in 4G LTE AMI in the cost of peak load management. This deployment showed that Massive MIMO beamforming over a 3.5 GHz band can readily penetrate the envelope of the high-rise residential buildings, and can provide 99.3%-meter successful rates to communicate with the gateway relay infrastructure that was once needed.

B. Dubai Integrated Utility Network (UAE)

It was a hybrid 5G Non-Standalone to Standalone migration of the Dubai Electricity and Water Authority (DEWA) in its integrated electricity and water distribution networks, with 850,000 devices or point of connections [22]. The deployment showed that network slicing can work well in managing the heterogeneous utility traffic types in a common physical infrastructure. An anomaly detection (powered by AI) which operates on the MEC servers was able to detect 847 previously unknown water network micro-leaks within the initial six months of operation which reflects projected water savings of 2.3 million liters per day. The techno-economic case to invest in 5g was confirmed by the case study, as the estimated 5-year ROI to invest in 5g was 340 percent compared to the 4G LTE, which had to be operated.

C. Bengaluru Multi-Utility Pilot (India)

The Bengaluru Smart City Limited pilot, created in partnership with BESCOM (Bangalore Electricity Supply Company) and Ericsson India, is the first multi-utility 5G implementation in South Asia, which brings together electricity, water and gas monitoring to a single 5G NSA network [23]. The system, which works in the 700 MHz 700 MHz spectrum over a long distance, allowing the system to penetrate large distances indoors in highly populated urban areas, the implementation of 45 km 2 pilot area has 320,000 connected devices. The rollout demonstrated critical insights into spectrum allocation to utility applications in the emerging urban markets, specifically: competition between consumer broadband and utility URLLC traffic on shared public 5G networks; a prompt reason to continue regulatory deliberation on utility spectrum licensing.

VIII. FUTURE RESEARCH DIRECTIONS

Although there are proven innovations in the use of 5G-enabled smart utilities to address utility management, there are still open research gaps that will bring changes to this area:

- 6G Integration Roadmap: This foreseen commercial use of 6G networks in the 2030s and terahertz (THz) communication features and the design of the air interface based on AI will necessitate a reconsideration of utility communication architecture. Studies are required to clarify support of migration pathway between 5G SA networks to 6G without losing investment on MEC infrastructure and network slice configurations [5].
- Digital twin synchronization: Digital twin models of utility infrastructure State synchronization Latency with sub-millisecond state synchronization ensures a high-fidelity model to realize what-if operational decision support. Studies of 5G-native state synchronization protocols that are optimized to digital twin applications are still emerging [11].
- Quantum-Resistant Security: Existing 5G cryptography primitives are at risk due to the potential threat of a quantum computing implementation. Empirical studies of the incorporation of post-quantum cryptography into 5G SUCI and slice authentication are needed to support the deployment of long-life utility infrastructures [13].
- Spectrum Coexistence and Dedicated Utility Spectrum: Regulatory frameworks of dedicated utility spectrum allocation of 5G band plans are not well developed. It needs to be researched to describe the interference behavior between shared 5G television spectrum deployments and those that use the spectrum by the private utility networks [19].

- Energy Harvesting in Massive IoT: Energy consumption of dense network of smart meters and sensors has a challenge of sustainability. Ambient backscatter communication studies with 5G and radio frequency energy harvesting on self-powered utility sensors are in line with the vision of smart cities sustainability [16].

IX. CONCLUSION

This paper provided an in-depth discussion of 5G-based projects to manage important power and utility infrastructure of a smart city. By discussing the building blocks of 5G architectures, the various technologies that make them possible, the performance of 5G technologies compared and contrasted with existing and previous technologies, security models, practical deployment experience, 5G portrays a qualitative step change in the communication capabilities of smart utility operators.

The service category URLLC, with sub-millisecond latency and 99.9999% reliability offers protection relay applications and real-time grid automation, which would have been impossible over cellular networks in the past. The mMTC feature is compatible with the high densities of connectivity needed to implement AMI pervasively in dense urban areas. Network slicing offers the logical separation that is required to allow secure coexistence of varied types of utility applications in common physical infrastructure. Practical implementation experience during pilot deployments in Seoul, Dubai, Bengaluru prove the efficiency increase of 3142% and latency of fault detection smaller than 18 milliseconds and large water savings results, caused by AI analytics at the network edge. Security issues would be inherent to critical infrastructure that is networked with 5G and can be mitigated by implementing layered mitigation measures including; isolation of network slices, authentication through blockchain schemes, and detection of anomalies by Artificial Intelligence.

Due to the ongoing worldwide coverage of 5G networking capabilities and the spectrum policy changes to incorporate utility-specific deployment model, the collaboration between 5G communication backbone and smart city utility management models will become cornerstones in next-generation resilience and sustainability initiatives in urban design. Further studies need to include 6G transition planning, quantum-resistant security integration/integration, and energy-harvesting IoT solution to support the emergent needs of this critical application domain.

REFERENCES

[1] R. Morello, S. C. Mukhopadhyay, Z. Liu, D. Slomovitz, and S. R. Samantaray, "Advances on sensing technologies for smart cities and power grids: A review," IEEE Sensors J., vol. 17, no. 23, pp. 7596–7610, Dec. 2017.

[2] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

[3] C. Saad al-Din, M. Alam, and S. Park, "Role of 5G in smart cities: Enabling technologies, challenges, and future prospects," Future Internet, vol. 13, no. 4, pp. 1–28, Apr. 2021.

[4] 3GPP, "System architecture for the 5G System (5GS)," 3rd Generation Partnership Project (3GPP), Technical Specification TS 23.501, Release 16, Dec. 2019.

[5] M. Bennis, M. Debbah, and H. V. Poor, "Ultrareliable and low-latency wireless communication: Tail, risk, and scale," Proc. IEEE, vol. 106, no. 10, pp. 1834–1853, Oct. 2018.

[6] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," IEEE Trans. Ind. Inform., vol. 7, no. 4, pp. 529–539, Nov. 2011.

[7] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[8] E. Hossain, M. Hasan, and V. K. Bhargava, "5G for smart energy: Advanced wireless technologies for smart grid applications," IEEE Commun. Mag., vol. 58, no. 9, pp. 62–69, Sep. 2020.

[9] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," IEEE Commun. Mag., vol. 55, no. 5, pp. 94–100, May 2017.

[10] Y. Liang, R. Yu, and W. Huang, "5G network slicing for smart grid communications: Architecture and resource allocation," IEEE Wireless Commun., vol. 26, no. 2, pp. 63–69, Apr. 2019.

[11] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[12] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence: Paving the last mile of artificial intelligence with edge computing," Proc. IEEE, vol. 107, no. 8, pp. 1738–1762, Aug. 2019.

[13] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in Proc. IEEE Conf. Stand. Commun. Netw. (CSCN), Helsinki, Finland, 2017, pp. 193–199.

[14] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," J. Netw. Comput. Appl., vol. 101, pp. 55–82, Jan. 2018.

[15] 3GPP, "Security architecture and procedures for 5G System," 3rd Generation Partnership Project (3GPP), Technical Specification TS 33.501, Release 15, Jun. 2018.

[16] ETSI, "Mobile edge computing (MEC); Framework and reference architecture," European Telecommunications Standards Institute (ETSI), Industry Specification Group (ISG) MEC, White Paper No. 11, 2016.

[17] IEC, "Communication networks and systems for power utility automation — Part 8-1: Specific communication service mapping (SCSM)," International Electrotechnical Commission (IEC), Standard IEC 61850-8-1, Ed. 2.0, 2011.

[18] IEEE, "IEEE Standard for Local and Metropolitan Area Networks — Bridges and Bridged Networks," Institute of Electrical and Electronics Engineers (IEEE), IEEE Std. 802.1Q-2018, Jul. 2018.

[19] J. Wu, S. Guo, J. Li, and D. Zeng, "Big data meet green challenges: Greening big data," IEEE Syst. J., vol. 10, no. 3, pp. 873–887, Sep. 2016.

[20] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," ACM Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 1–33, Jun. 2011.

[21] Korea Electric Power Corporation (KEPCO), "Smart grid roadmap and deployment update 2022," KEPCO, Seoul, South Korea, Tech. Rep. KEPCO-SG-2022, 2022.

[22] Dubai Electricity and Water Authority (DEWA), "Annual sustainability report: Smart grid and digital transformation," DEWA, Dubai, UAE, Tech. Rep., 2022.

[23] Bengaluru Smart City Limited, "5G multi-utility pilot deployment report: Phase I results," BSCL, Bengaluru, India, Internal Tech. Rep. BSCL-5G-2023, 2023.