sensors

*Review*

# Communication Technologies for Smart Grid: A Comprehensive Survey

**Fredrik Ege Abrahamsen [1,*], Yun Ai [2] and Michael Cheffena [2]**

[1] Department of Electronic Systems, Faculty of Information Technology and Electrical Engineering, NTNU–Norwegian University of Science and Technology, 2815 Gjøvik, Norway
[2] Department of Manufacturing and Civil Engineering, Faculty of Engineering, NTNU–Norwegian University of Science and Technology, 2815 Gjøvik, Norway; aiyun@alumni.chalmers.se (Y.A.); michael.cheffena@ntnu.no (M.C.)
* Correspondence: fredrik.e.abrahamsen@ntnu.no

**Abstract:** With the ongoing trends in the energy sector such as vehicular electrification and renewable energy, the Smart Grid (SG) is clearly playing a more and more important role in the electric power system industry. One essential feature of the SG is the information flow over high-speed, reliable, and secure data communication networks in order to manage the complex power systems effectively and intelligently. SGs utilize bidirectional communication to function whereas traditional power grids mainly only use one-way communication. The communication requirements and suitable techniques differ depending on the specific environment and scenario. In this paper, we provide a comprehensive and up-to-date survey on the communication technologies used in the SG, including the communication requirements, physical layer technologies, network architectures, and research challenges. This survey aims to help the readers identify the potential research problems in the continued research on the topic of SG communications.

**Keywords:** review; survey; smart grid; smart grid technologies; smart grid communication; wireless communications; wired communication; smart grid security

check for updates

**Citation:** Abrahamsen, F.E.; Ai, Y.; Cheffena, M. Communication Technologies for Smart Grid: A Comprehensive Survey. *Sensors* **2021**, *21*, 8087. https://doi.org/10.3390/s21238087

Academic Editor: Fco Javier Rodríguez

Received: 15 September 2021
Accepted: 26 November 2021
Published: 3 December 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

## 1. Introduction

Today's method for the generation and distribution of electric power was designed and constructed in the last century and has remained unchanged since. The traditional power grids are primarily radial and built for centralized power generation. Reliability is ensured by having excessive capacity and one-way power flow from the power plant to the consumer through high voltage transmission lines, often over long distances. With the demand for electric energy continuously increasing, and the existing conventional grid being at the end of its life cycle, increasing amounts of distributed renewable energy sources (RES) and energy storage systems (ESS) require new ways of managing and controlling the power grid and distributing the power in a more efficient, effective environmentally sustainable and economical manner. The next-generation power grids are often referred to as Smart Grids (SG). SGs are achieved by overlaying a hierarchical communication infrastructure on the power grid infrastructure [1–4].

Since 1 January 2019, most end-users in Norway should have installed smart electricity meters as part of the implementation of Advanced Metering Infrastructure (AMI) in the Norwegian power grid [5]. By the end of 2020, 3.2 million, or 99% of the electricity meters in Norway were smart meters [6]. In EU, it was committed by the member states to achieve a rollout of close to 200 million smart meters for electricity by 2020. About 71% of European consumers then will have a smart electricity meter installed [7]. Globally it is expected that 800 million smart meters will be installed by 2020 [8]. The installation of these metering devices can be seen as one of the first steps toward a smarter grid system, as implementing a SG is not a one-time event, but rather an evolutionary process. The smart meters have the ability to collect and report consumption data to the utilities provider several times per hour, rather than the consumer having to report every month manually. The smart meters also open up for the consumer to feed the grid with electricity from, i.e., solar panels or electric vehicles. Other possibilities with smart metering are a higher degree of monitoring and control of the grid, automatic fault detection, and reports [1,9].

The rest of the paper is organized as follows: Section 2 gives an overview of Smart Grid infrastructure, domains, architecture, and applications. Section 3 presents Smart Grid communication technologies and network structures. Section 4 addresses challenges of Smart Grid communications, and the privacy and security of Smart Grid communication. The organization of this paper is summarized in Figure 1.

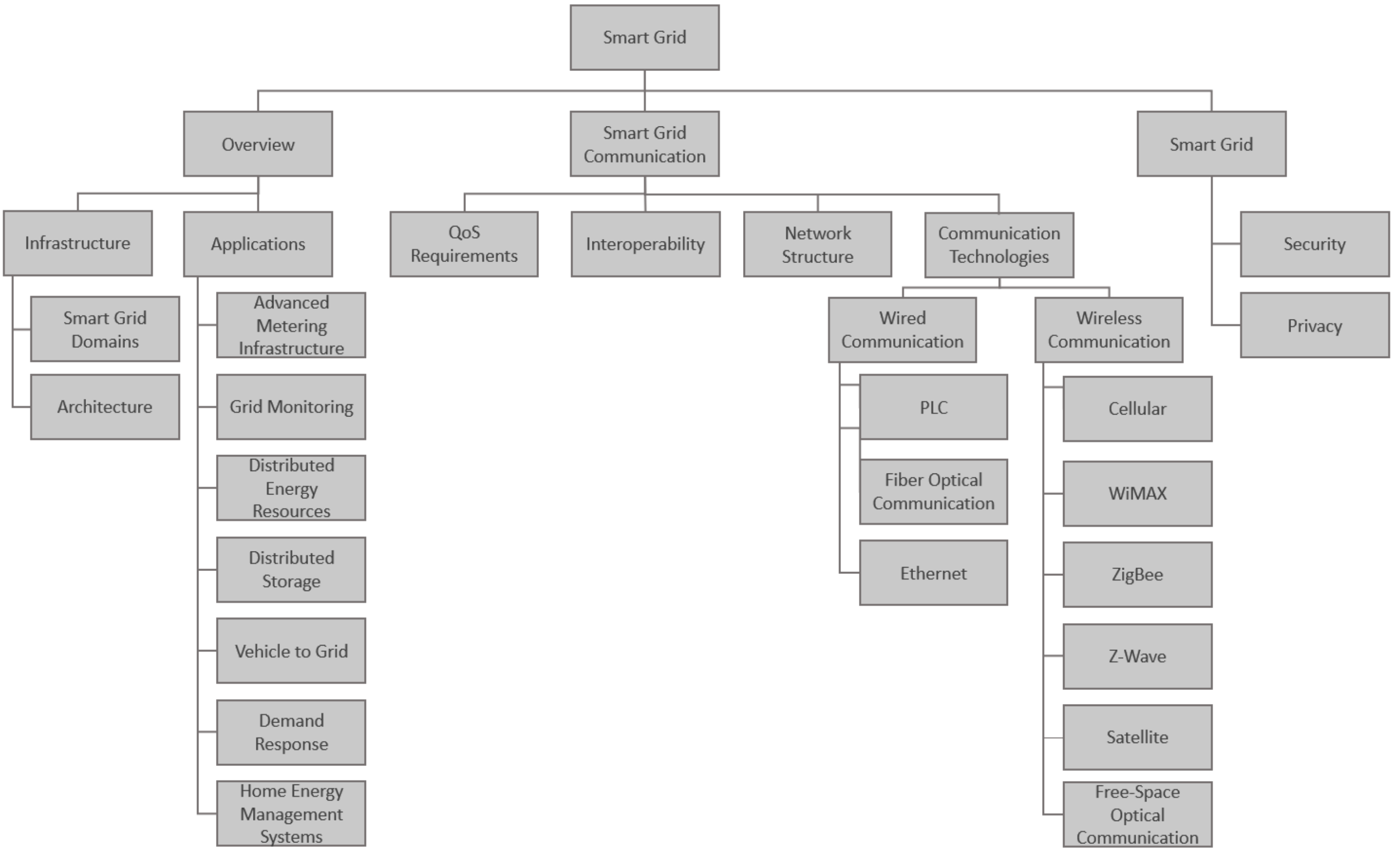

**Figure 1.** The structure of the paper.

## 2. Overview of Smart Grid

Communication play an important role in SGs, as one of the most significant differences between traditional grids and SGs is two-way communication. Traditional power grids only provide one-way communication between the utilities and the customer, whereas SGs provide two-way communication [3,10]. This enables use of distributed smart sensors, distributed power generation, real-time measurements and metering infrastructure, and monitoring systems. Information exchange is of great importance for the SG to provide reliable power generation and distribution. Following is an overview of SG infrastructure, domains, network architecture, and SG applications.

### 2.1. Smart Grid Infrastructure

Both international and national organizations have developed roadmaps, defined standards and definitions on what makes a power grid a Smart Grid [9,11–16]. There is no single definition of what a Smart Grid is, however common in the definitions is the emphasis on communication for measurements, monitoring, management, and control. Communication plays an essential role in providing reliable, efficient and secure power generation, transmission, and distribution. The communication systems provide information exchange between the distributed sensing equipment, monitoring systems, and data management systems. These solutions require fast communications as the generation, delivery, and consumption all happen at the same time. With the introduction of distributed energy resources and energy storage systems, the importance of fast and reliable communication increases. The expectations from end-users also change, with real-time information on electricity prices, customers feeding the grid with electricity, and electric vehicles acting as batteries in the grid. A key goal for SGs are reduced cost and environmental impact, and maximizing reliability, resilience, and stability [9]. The smart meter is a key component of the SG infrastructure, and part of the Advanced Metering Infrastructure (AMI). AMI is responsible for enabling a reliable and secure high speed two way communication between smart meters at the end-user, and data control centers at the utilities companies for monitoring and control [11,17,18]. The full benefit of the SG infrastructure is achieved when smart meters, sensors, and measuring devices located throughout the power grid communicate in order to ensure stability, detect, predict, and prevent faults, forecast load changes and facilitate demand response [19]. Table 1 shows the main differences between a traditional grid and a SG.

**Table 1.** Comparison of traditional power grid and smart power grid [3].

| | **Traditional Grid** | **Smart Grid** |
|---|---|---|
| Information flow | One-way communication | Two-way communication |
| Power generation | Centralized power generation | Distributed power generation |
| Grid topology | Radial | Network |
| Integration of distributed energy sources | Low degree | High degree |
| Sensors | Low degree | High degree |
| Monitoring | Manual monitoring | Self-monitoring |
| Outage recovery | Manual restoration | Self-reconfiguration |
| Testing | Manual | Remote |
| Ability to control | Limited | Pervasive |
| Efficiency | Low | High |

### 2.1.1. Smart Grid Domains

SGs are complex systems, interfacing the power grid with communication technologies by deploying a large number of interconnected components for measuring, controlling, and monitoring. SGs consists of different domains responsible for different parts of the SG infrastructure [20,21]. To structure the different areas of a SG environment, The National Institute of Standards and Technology (NIST) [12] proposed seven domains of SG with electrical interfaces and communication interfaces in its conceptual model for SG information networks in 2009. The conceptual model has later been updated with more communications and electrical interfaces to better reflect the increase in distributed energy sources and automation of distribution systems [14,22]. Table 2 shows the definition of these domains. The domains are; Customer, Distribution, Transmission, and Generation including DER, Markets, Operations, and Service Providers. The first four are related to transmission of electricity on the power grid.

**Table 2.** Smart Grid domains, electrical and communication interface [23].

| Domain | Communication Interface | Electrical Interface |
|---|---|---|
| Market | Service provider, Operations, Generation, Transmission, Distribution, Customer | None |
| Operations | Markets, Service provider, Transmission, Distribution, Customer, Generation | None |
| Service provider | Markets, Operations, Customer, Distribution, Generation | None |
| Transmission | Markets, Operations Generation, Distribution | Generation, Distribution |
| Distribution | Operations, Transmission, Customer, Service Provider | Transmission, Customer |
| Customer | Markets, Operations, Service provider, Distribution | Distribution, Generation |
| Generation incl. DER | Markets, Operations, Transmission, Customer | Transmission, Customer |

- **Market Domain:** Grid assets and services are bought and sold within the domain. The market domain handles actors such as market management, wholesale, trading, and retailing. The market domain communicates with all other domains in the SG. Communication between market domain and the energy supplying domains are critical, due to the need for efficient matching of production and consumption [14].
- **Operations Domain:** The domain is responsible for operations of the grid. Including monitoring, control, fault detection and management, grid maintenance, and customer support. These are typically the responsibilities of the utilities today. With SGs more of these responsibilities will move over to service providers [12,13].
- **Service Provider Domain:** Actors in the domain support business processes of power producers, distributors, and customers. Ranging from utility services such as billing to management of energy use and generation. The communication interface is shared with the Generation, Distribution, Markets, Operations, and Customer. Communication with the operations domain is critical to ensure system control and situational awareness [12,13].
- **Generation Domain:** The power generation domain is responsible for power generation in bulk or non-bulk quantities. This can be from, for example, fossil fuels, water, wind, or solar. For the case of Norway, this is typically hydropower, these are grid-connected power generation stations. Power generation include distributed energy resources. SGs allow for end-users to also operate as producer of electrical energy, for premise use, storage, or for resale. [13,24]. With SGs, power generation is no longer limited to large fossil or hydroelectric power facilities feeding the transmission grid. SGs allow for smaller scale distribution-grid-connected power generation. This can be wind power parks, solar parks, photovoltaic panels mounted on end-users roof-tops, or electric vehicles feeding the grid [13,25]. Communication with the transmission and distribution domains are important to maintain energy delivery to customers [12,13].
- **Transmission Domain:** The power transmission domain is responsible for the transfer of power from the power generation source to the distribution system. The transmission domain typically consists of transmission lines, substations, energy storage systems, and measurement and control systems. The transmission system is typically monitored and controlled through a Supervisory Control And Data Acquisition (SCADA) system which communicates with field and control devices throughout the transmission grid [12,13].

- **Distribution incl. DER Domain:** This domain is the connection between the transmission and the customer domain. The distribution domain may include DERs located at customer or at grid operator. In a SG environment, the distribution domain communicates with the market domain due to the market domains potential to affect local power consumption and generation [12–14].
- **Customer Domain:** The customer or end-user could be private, commercial or industrial. In addition to consume the energy, the customer could also generate and feed the grid with excess energy or stored energy. In cases where the customer generate and deliver energy consumer is referred to as a prosumer [14,26].

Reliable communication is required for information exchange between the different domains to ensure reliable operations of the power grid and its applications. Similar to NIST in the US, in Europe, the Smart Grid Coordination Group defined its Smart Grid Architecture Model [11,27,28]. There are similarities between the two models, the domains are the same. In addition to domains this model is also divided in layers and zones. This is a three dimensional model consisting of five interoperability layers (Business, Function, Information, Communication, and Components). The two dimensions are divided in domains (Generation, Transmission, Distribution, DER, and Customer Premises), and zones (Process, Field, Station, Operation, Enterprise, and Market). Table 3 shows the different layers, dimensions and zones of SGs.

**Table 3.** Overview of SG communication layers [20].

| **Application Layer** | **Power Transmission and Distribution Applications** | | **Customer Applications** |
|---|---|---|---|
| Communication Layer | Wide Area Network | Neighborhood Area Network/Field Area Network | Premise Area Network (Home Area Network, Building Area Network, Industrial Area Network) |
| Power Control Layer | Power monitoring, control, and management systems | | |
| Power System Layer | Power Generation and Transmission | Power Distribution | Customer |

### 2.1.2. Architecture

What separates Smart Grids from traditional electrical grids are the interaction and communication between the different domains. The SG infrastructure can be structured by dividing it in four layers: the application layer, the communication layer, the power control layer, and the power system layer. On the customer side, the application layer enables various applications such as home automation and real-time pricing. On the grid side: automation of grid and power distribution applications. The communication layer is important in distinguishing Smart Grids from traditional power grids, and in enabling SG applications. It is divided into three categories classified by geographic area (Wide Area Network, Neighborhood Area Network/Field Area Network, and the Premise Area Network). Depending on the type of network, different communication technologies are used. The power control layer enables management, control and monitoring of the power grid, and utilizing equipment such as switches, sensors, and metering devices. The power system layer handles power generation, transmission/distribution, and the customer premises.

## *2.2. Smart Grid Applications*

SG applications for monitoring and grid management include Advanced Metering Infrastructure (AMI), Distributed Automation (DA), Distributed Generation (DG), Distributed Storage, Home Energy Management Systems (HEMS), Demand Response (DR), and Supervisory Control And Data Acquisition (SCADA). All depend on reliable wired and wireless communication interfaces to operate in the SG infrastructure.

**Advanced Metering Infrastructure (AMI)**

SGs are considered as one of the largest potential IoT network implementations with smart meters and wireless smart sensors placed throughout the grid, and smart appliances communicating with each other to ensure reliable and efficient power generation and distribution. The advanced metering infrastructure consists of physical and virtual components, including sensors, monitoring systems, smart meters, software, data management systems, and communication networks. AMI is responsible for collecting, analyzing, and storing metering data sent from sensors and monitoring systems and smart meters at the end-user to the utility companies for billing, grid management, and forecasting. SG interactions based on measured data and communication from sensor networks [29,30].

The smart metering devices installed on the customer premises use different technologies for communicating. These vary depending on what manufacturer smart meter the utilities company are installing, and the application. For large apartment buildings, the metering devices can be connected to the master device by RS-485 [31]. As illustrated in Figure 2, the metering devices can also be directly connected to the Head-End System (HES) through 3G/4G/5G or fiber networks, so-called end-to-end connection. The master device uses 3G/4G/5G, Ethernet, fiber optics, or power line communication (PLC) to communicate with the head-end system at the utilities company. Inside the premise area, the smart meter communicates through the HAN-port, the communication is based on IEC 62056-7-8, with RJ45 connector and M-Bus interface. From this port, other third-party equipment can be installed i.e., HEMS or household appliances [32].

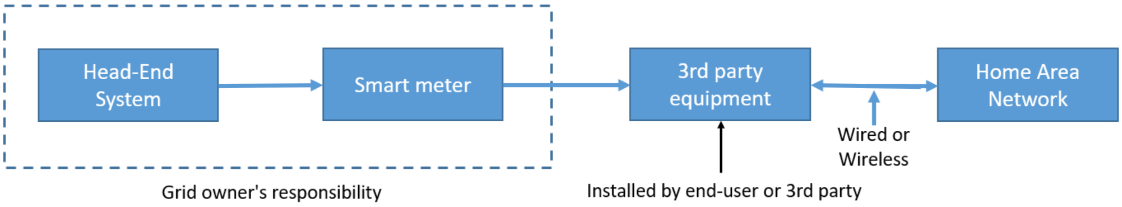

**Figure 2.** Smart metering architecture.

**Grid monitoring**

Grid monitoring is necessary to ensure that the power quality is maintained throughout the power grid. Frequency, voltage, and waveform must stay within defined limits, and consequences for low power quality are reduced lifetime of sensors, devices, and appliances connected to the power grid. Grid monitoring is performed by smart sensors placed throughout the grid, AMI, and integration of SCADA [33]. The SCADA functions are enhanced from the traditional grid due to fast two-way communication and implementation of large numbers of sensors. For transmission line monitoring, wireless smart sensor nodes are distributed along the transmission line, exchanging measurements to the neighboring nodes. The nodes forward the measurements to a central collection site over NAN or WAN. The central is connected to a base station with low latency, high bandwidth, and low cost links [34]. To ensure uninterrupted power delivery continuous monitoring is required. Fast outage identification, management, and restoration systems can be achieved by interfacing the outage management systems with SCADA, AMI, and geographical information systems. Integration of AMI and smart meters can give notifications or the last gap reports to outage management systems before the customer notices the outage, thus helping in reducing trouble-shooting time and restoration time [34]. These systems for status monitoring of the SG infrastructure down to individual components help to detect, predict, and respond to faults faster. The result is better management, more accurate optimization of resources, better and faster identification of faults in the grid, reduction in troubleshooting-time, and improved reliability [29,30].

**Distributed Energy Resources (DER)**

Distributed energy resources have a substantial potential at generating electricity at the load end. DER include solar photovoltaic panels, windpower and biomass. Two-way communication in the AMI enable the end user to sell surplus energy, and feeding it back to the power grid [35,36]. Due to the intermittent characteristics of renewable energy sources (RES), the increasing utilization of renewable energy sources in the power grid, will result in more frequency and voltage fluctuations [4,37]. Thus, fast acting smart sensing and protection equipment, as well as fast reliable communication become more important to maintain system balance and to monitor and coordinate DERs in the grid [4,37–40].

**Distributed Storage**

Distributed storage is an integral part of the SG infrastructure. Energy storage systems should be located near RES or end user to mitigate problems related to variations in energy production from RES [41]. Fast response to stability issues in the grid are dependent on fast and reliable communication links in the SG. Distributed storage in combination with DER can improve the utilization RES and demand response [40,42].

**Vehicle to Grid (V2G)**

It is clear that the electrification of vehicles is becoming an ongoing trend around the globe now, which implies the frequent interaction between power grid and vehicles in the future. Electric vehicles (EVs) and chargers connecting a vehicle to a grid network can utilize the stored energy in the vehicle batteries and feed it back to the grid when necessary. EVs in the power grid can be used for power balancing by providing fast response high power. EVs can reduce the energy demand in peak load hours by consuming, storing, and returning energy when needed. EVs can also be used as back up power or in islanded operation if connection to the grid is not possible [43,44]. These applications require bidirectional communication between the utilities and the EVs.

**Demand Response (DR)**

AMI and communication between end-user and the utilities companies give ability for demand response (DR) from the consumer side, or the utility side in predefined cases. From the consumer side, demand response gives the end-user the ability to monitor its energy consumption and production. The end-user can, for example, alter their habits, and shift the demand to off-peak hours in response to dynamic pricing programs such as time of use, real time pricing, critical peak timing or to incentivize payment when grid reliability is low [45–47]. Demand response can also be an automated part of home energy management systems, where certain appliances or lighting can be turned off to reduce consumption [48]. Demand side management or demand response can be used to reduce power constraint, shift peak load, reduce distribution losses, and regulate voltage drops and avoid or postpone the need for building new power lines [29,49].

**Home Energy Management Systems (HEMS)**

HEMS is used to enable demand response applications. HEMS systems permit the end-users to monitor, control, and manage the power consumption. These systems are comprised of smart appliances, sensors, smart meters, and in-home displays, and include applications for example home automation, temperature zone setting, water temperature, and controlling electricity use depending on real-time pricing information, etc. Appliances and sensors connects to HEMS through sensor networks and to the utility companies AMI through the smart meter HAN interface [32,34].

## 3. Smart Grid Communication

From the previous section we can see that SGs are highly dependent on information flow and communication between different entities in different networks. Communication is one of enabling technologies of SG. As the number of sensors increase, the amount of data coming to and from the utility increases.

### *3.1. QoS Requirements for Smart Grids*

SG applications result in increased data, these applications have different QoS requirements. Secure bi-directional communication that satisfies the different SG applications' QoS requirements is essential [34]. Control, management, and automation applications such as demand response (DR) and substation automation require low latency and high reliability to ensure grid operation. Other applications such as meter readings can tolerate a higher latency, but still require high reliability [34,50]. Table 4 lists QoS requirements for different SG applications.

**Table 4.** Smart Grid QoS requirements [50].

| Smart Grid Application | Data Rate | Latency | Reliability |
|---|---|---|---|
| Smart Metering | Low | High | Medium |
| SCADA | Medium | Low | High |
| Substation Automation | Low | Low | High |
| DER | Medium | Low | High |
| DR | Low | Low | High |

### *3.2. Interoperability*

With the different equipment interconnected in the SG, interoperability must be ensured for seamless communication [13]. Interoperability ensures that if any device supplied by one manufacturer with a similar device from another manufacturer, the application will continue to operate as before [51]. Interoperability must also be ensured for legacy and evolving communication protocols. Standardization of communication is imperative to achieve a fully connected SG. The IEC 61850 standard offers interoperability of devices across manufacturers, and was initially introduced as a standard for substation communication. In recent years this standard has been utilized for different equipment such as smart meters, virtual power plants, and V2G [51–53].

### *3.3. Communication Network Structure*

A defined communications framework is necessary in this infrastructure. It is crucial to have clearly defined standards to ensure reliable, efficient and secure communication throughout the system [54]. The different network types in the communications layer mentioned above have all different requirements when it comes to data rate and coverage distance, and the chosen communication technology must support these specific requirements, which are summarized in Figure 3 and Table 5. The networks utilize different technologies for communication, both wireless and wired. The premise network (HAN, NAN, or IAN) is closest to the end-user, and enables information and communication flow between home appliances or for example heating, ventilation, and air conditioning (HVAC) systems within the end-user premise. Multiple HANs connects to a NAN. The NAN collects information, and enables communication to the WAN. An illustration of different networks in an SG are depicted in Figure 4. The WAN handles communication of metering information from the end-user to the utilities companies [55].

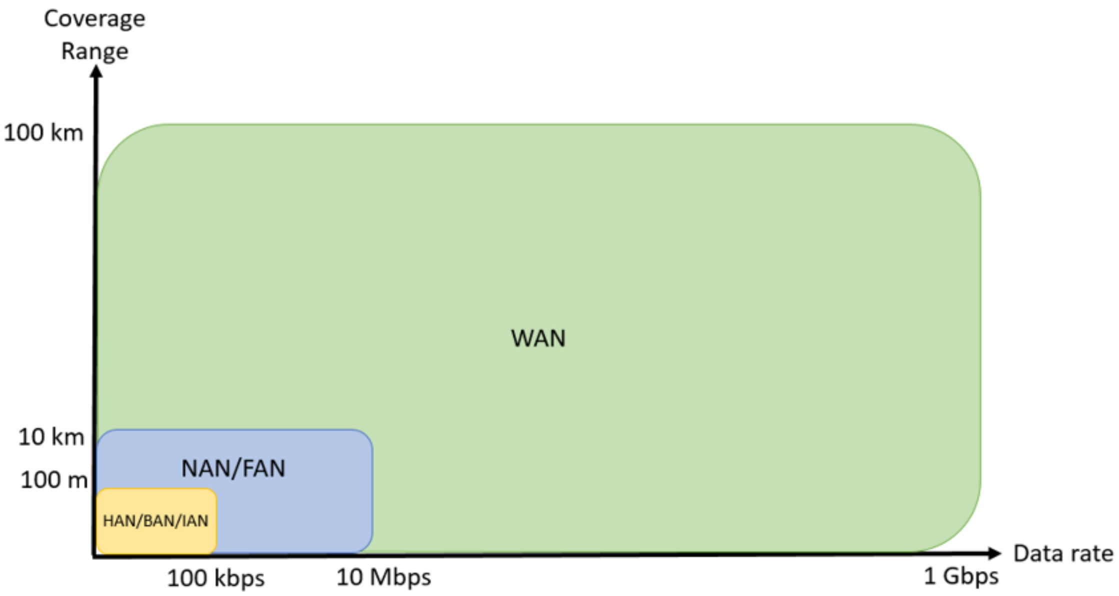

**Figure 3.** Data rate and communication range requirements in SG hierarchy [20].

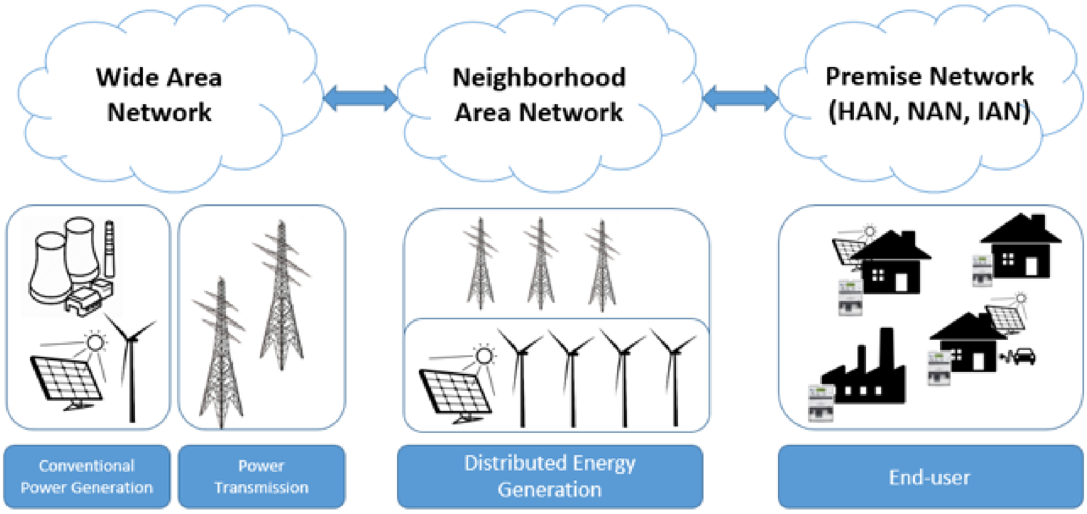
Wide Area Network
Neighborhood Area Network
Premise Network (HAN, NAN, IAN)
Conventional Power Generation
Power Transmission
Distributed Energy Generation
End-user

**Figure 4.** Networks in SG.

**Table 5.** Overview of network types and requirements [20].

| Network Type | Coverage | Data Rate Requirements | Data Rate | Technology Alternatives |
|---|---|---|---|---|
| WAN | 10–100 km | High data rate. Devices such as routers and switches. | 10 Mbps −1 Gbps | Wireless: WiMAX, 3G,4G,5G.<br>Wired: Ethernet, Fiber Optic |
| NAN/FAN | 10 m–10 km | Highly dependent on node density and topology. | 100 kbps −10 Mbps | Wireless: ZigBee, Wi-Fi, WiMAX, Cellular.<br>Wired: Power Line Communication |
| HAN/BAN/IAN | 1–100 m | Dependent on application. Generally low data rate required. | 10–100 kbps | Wireless: ZigBee, Z-wave, Wi-Fi.<br>Wired: Ethernet, HomePlug, M-Bus |

### Wide Area Network

A WAN forms the backbone of the communication network in the power grid. It connects smaller distributed networks such as transmission substations, control systems and protection equipment, e.g., Supervisory Control and Data Acquisition (SCADA), Remote Terminal Unit (RTU), and Phasor Measurement Unit (PMU) to the utility companies' control centers [20,56]. Other terms used for the WAN is the backbone network or Metropolitan Area Network [20]. WAN applications require a higher number of data points at high data rates (10 Mbps–1 Gbps), and long-distance coverage (10–100 km). Real-time measurements are taken throughout the power grid by measurement and control devices and sent to control centers. In reverse, instructions and commands are sent from control centers to the devices [56]. This communication requires both a high degree of distance coverage and speed to maintain stability. Suitable communication technologies for this application are PLC, fiber optic communication, cellular, or WiMAX. Satellite communication can be used as backup communication or in remote locations [20,57].

### Neighborhood Area Network/Field Area Network:

The Neighborhood Area Network (NAN) and Field Area Network (FAN) are networks within the distribution domain, both enable the flow of information between WAN and a Premise Area Network (HAN, BAN, IAN). The NAN connects premises networks within a neighborhood via smart meters at the end-user. The NAN enable services such as monitoring and controlling electricity delivery to each end-user, demand response and distribution automation. The area NAN/FAN covers can in some cases be large, one of the features of NAN/FAN is communication between intelligent electronic devices (IEDs). The data in a NAN/FAN is transmitted from a large number of sources to a data concentrator or substation. This requires a high data rate and large coverage distance. For the existing grid infrastructure in the NAN/FAN covered areas, it in most cases not possible to make extensive alterations to the infrastructure. Because of the varying nature of the physical environment of which the NAN/FAN operate, coverage requirements, etc., different technologies for communication are used. When the coverage requirements are lower, standards from NAN can be applied, if longer coverage is required, other technologies will be more suitable. The communication technologies used therefore have to be adapted to each specific situation. Both wired and wireless technologies are used in NAN/FAN, and the different communication technologies should be complementary. As distributed energy generation are deployed, these are connected to the NAN/FAN. Communication technologies such as ZigBee, Wi-Fi, Ethernet, or PLC are widely used in these networks [20,57,58].

### Premise Area Network

The Premise Area Network divides into three sections depending on the environment, HAN (Home Area Network), Building Area Network (BAN), and IAN (Industrial Area Network). These are wired or wireless networks within the end-user's premise. The purpose of the HAN is to provide communication between for example the smart meter and home automation, appliances, Home Energy Management Systems (HEMS), solar panels, or electric vehicles. BAN and IAN are commercial and industrial focused and communicate typically with building automation systems such as heating and ventilation or energy management systems. These applications do not require large coverage, high speed, or high data rate, and can be managed with low power, low-cost technologies such as Power Line Communication (PLC), Wi-Fi, or ZigBee [57]. The required bandwidth in HANs vary from 10 to 100 kbps for each device, depending on function. The premise networks should be expandable to allow for the number of connected devices to increase [59]. Other applications for the smart metering devices within the premise area are delivering information such as power and real-time price information to the end-user through HEMS. The end-user can then make decisions whether to use appliances during high price periods or wait for lower price. This can in turn help with peak demand reduction and load shifting [60].

### *3.4. Smart Grid Communication Technologies*

Communication technologies utilized in SG can as mentioned be wired or wireless. Most power systems use a combination of different wired and wireless technologies, depending on the infrastructure. Several factor that has to be taken into account when deciding on communication technology used in SGs and smart metering. Wireless communication alternatives have some advantages over wired communication, such as low cost and connectivity in inaccessible areas. A number of factors have to be considered for each different case to decide on communication technology. Requirement include aspects such as geographical topography, technical and operational requirements and cost [61]. Wireless communication is less costly to implement in a complex infrastructure and ease of installation in some areas. Wired connection will not necessarily struggle with interference issues as wireless solutions may do. Both types of communication are necessary in SG environments. The technology that fits one environment may not be suitable in a different environment. Tables 6 and 7 gives a summary of wired and wireless communication technologies for SG. Following is a overview of some of the wired and wireless communication technologies used for SGs, together with advantages and limitations.

#### 3.4.1. Wired Communication

**Power Line Communication (PLC)**

Power line communication utilizes the power transmission lines to transmit data. High frequency signals from a few kHz to tens of MHz are transferred over the power line [62]. The initial cost of PLC is lower since it uses the existing power line infrastructure. The technology is mature, and has already been in use for decades for commercial broadband and is highly reliable. PLC provide high throughput and low latency which makes it suitable for SG communication in densely populated areas [63]. Power line communications divides into narrowband and broadband PLC. Narrowband PLC (NB-PLC) is operating at 300–500 kHz with a data rate up to 10–500 Kbps and a range up to 3 km. This is further divided into Low Data Rate Narrowband PLC and High Data Rate Narrowband PLC. Low data Rate Narrowband PLC is single carrier based, with a data rate up to 10 kbps. High Data Rate Narrowband PLC is multi carrier based with a data rate up to 1 Mbps. Broadband PLC (BB-PLC) operates between 1.8 and 250 MHz with a data rate up to 300 Mbps. Power Line Communication can be used in nearly all parts of a SG environment, from home appliances in low voltage to grid automation in high voltage [64]. The noise created by power electronics components in the channel is a major concern with this form of communication [65–67]. Data distortion around transformers, and the need to bypass these using other communication techniques is another disadvantage with PLC [59]. Extensive field measurements show that the characteristics of PLC channel differ significantly from one environment to another, which leads to varying performance [68]. The large deployment of power cables also makes the combination of PLC technique with other communication technologies (e.g., radio frequency (RF), visible light communication (VLC), etc.) an attractive approach to extend the communication coverage, thus enabling a variety of applications such as smart home, Internet of Things, etc. [69–71]. HomePlug is a type of power line communication specifically developed in-home applications and appliances. HomePlug Green PHY (HPGP) uses PLC technology, and is developed and marketed towards HAN applications. It has a data rate up to 10 Mbps, and operates in the 2 MHz–30 MHz spectrum (BB-PLC) [72,73].

**Fiber Optical Communication**

Fiber optical communication is well suited for control and monitoring, and backbone communication in WANs, although it is more expensive than other alternatives it has the advantages of long range, high bandwidth, and high data rate, and not being susceptible to electromagnetic disturbances. Limitations of fiber optic communication is the number of access points. Fiber optics are most commonly used for backbone communication, and to connect substations to the utility companies control centers [21,34,74].

**Ethernet**

Suited for communication in WAN between substations and control centers. Advantages with this form of communications is its high availability and high reliability. Ethernet is also used in HAN for the communication between smart meters and home central.

### 3.4.2. Wireless Communication

**Cellular Communication**

Cellular communication can be used where continuous communication is not required. Advantages with using cellular communication technology is that it is already existing, it has widespread coverage, low cost, and high security. One disadvantage with cellular communication is the fact that the network is shared with many other users, this can in some cases result in network congestion. Universal Mobile Telecommunications System (UMT), Long-Term Evolution (LTE), LTE-Machine Type Communication (LTE-M), and Narrowband IoT (NB-IoT) are technologies used for communication in SGs. The last two were specifically developed for IoT applications. LTE-M and NB-IoT are both low power wide area networks. LTE-M offers higher data rate, but require more bandwidth [75–77].

The fifth generation mobile communication network (5G) utilizes wide frequency range including millimeter wave (mm) spectra and operate at higher frequencies than LTE/4G system. Additionally, the bandwidths of 5G are higher than previous generations. The advantages of 5G over earlier generations include higher data rate and low communication latency, improved security and reliability, low power consumption, and ability to connect a higher number of devices. This makes 5G suitable for SG infrastructure [37,40,78]. 5G supports ultra-Reliable Low Latency Communication (uRLLC) which is suitable for applications with strict requirements to low latency and high reliability e.g., mission critical applications such as remote control of digital substations [53,79,80]. A comprehensive review on the use of 5G for SGs with the future roadmaps and challenges is provided in [81]. The security for SGs in future generation (5G and beyond) mobile networks is discussed in [78].

**WiMAX (IEEE 802.16)**

Worldwide inter-operability for Microwave Access (WiMAX) is a short range wireless communication technology based on the IEEE 802.16 standards with a data rate up to 70 Mbps and a range of 50 km. WiMAX operates in two frequency bands, 11–66 GHz for line-of-sight, and 2–11 GHz for non-line-of-sight communication [82]. The physical and MAC layers are defined by IEEE 802.16. The physical layer provides Orthogonal Frequency-Division Multiple Access (OFDMA) and Multiple-Input Multiple-Output (MIMO) antenna system providing increased non-line-of-sight capabilities. The Media Access Control (MAC)-layer enables Data Encryption Standard (DES) and Advanced Encryption Standard (AES) encryption to ensure secure and reliable communication. The MAC-layer also enables power saving techniques, such as sleep and idle [83]. WiMAX is scalable and can be set up as networks on local or regional level. WiMAX is well suited for sensors and meters provided sufficient numbers of nodes in the area. One limitation with WiMAX is that coverage becomes highly limited due to signal losses (e.g., rain attenuation, blockage, etc.) [84].

**ZigBee (IEEE 802.15.4)**

ZigBee is an open wireless mesh network standard based on the IEEE 802.15.4 standard. It is a short range, low data rate, and energy efficient technology. ZigBee operates on four different frequency bands, 868 MHz (20 kbps per channel), 915 MHz (40 kbps per channel), and 2.4 GHz (250 kbps per channel) [85,86]. ZigBee has mesh capabilities and a coverage range from 10 to 100 m [54]. Mesh networks are decentralized, where each node are self-manageable, and can re-route, and connect with new nodes when needed. This makes ZigBee well suited for use in HAN applications such as remote monitoring, home automation, consumer electronics and smart meter readings [87,88]. A ZigBee mesh network is constructed of three different types of nodes; Coordinator, Router, and End-Device. ZigBee uses AES-128 access control to manage a high level of security. Because of the low transmission power level, this technology is vulnerable to multipath distortion, noise and interference [86]. ZigBee operating on the 2.4 GHz band is also affected by interference from technologies such as Wi-Fi, USB, Bluetooth, and microwave ovens as these operate on the same unlicensed frequency band [89–91].

#### Z-Wave (IEEE 802.15.4)

Z-Wave is a proprietary communications standard intended for remote control of applications in residential and commercial areas. In Europe, it operate on 868 MHz with a data rate of 9.6 kbps, and on 2.4 GHz with a data rate up to 200 kbps. Range-wise, Z-Wave typically has around 30 m indoor range, and up to 100 m outdoors. Z-Wave is short range, low data rate, and low cost alternative. Z-Wave can also be organized as mesh network, increasing the range [86]. Similar to ZigBee, Z-Wave also uses AES-128 encryption standard to maintain a high level of security in the network [92].

#### Wi-Fi (IEEE 802.11)

Wi-Fi technology, based on the IEEE 802.11 family of standards, is a wireless networking technique that is being widely used for Internet access. It can also be a good choice in the context of smart grid, which enables consumers to monitor the improvement their energy use [93]. Wi-Fi solutions are already being utilized in a number of devices that contribute to the so-called smart home. For instance Wi-Fi is used in thermostats, appliances, and new smart energy home devices that will connect them all together to help consumers manage their own energy consumption [93–95].

#### Satellite Communication

Satellite communication can play an important role in SG communication in rural areas without cellular coverage, or as a backup solution for other communication technologies [96]. Examples of areas of use for satellite communication are control and monitoring of remotely located substations [97].

#### Free-Space Optical (FSO) Communications

The demand for higher data rates requires broader bandwidth for communication system. Among different potential technologies, free-space optical (FSO) communication is one of the most promising technologies addressing the problem of large bandwidth and data rate requirements, as well as the "last mile bottleneck". The FSO system functions by transmitting modulated laser light through the air between the transmitter and receiver. More specifically, the signal is transmitted using a lens or parabolic mirror by narrowing the light and projecting it towards the receiver. The emitted light is then picked up at the receiver with a lens or mirror. Subsequently, the received light is focused on an optical detector and converted to electrical signals for further information extraction [98]. Besides the advantages of large data rate with unlicensed spectrum, the FSO communication is also considered to be a more secure technique than the RF communication [99–102]. Thanks to the various advantages of FSO communications, FSO link can be part of the backhaul communication network for rural or remote substations monitoring applications. In [103], the FSO system based on a microring resonator (MRR) with the ability to deliver up to gigabit (line-of-sight) transmission per second is proposed for the two SG applications (AMI and DR). The experimental results demonstrate up to 10 times bandwidth improvement over the radius as large as 600 m and maintain receive power higher than the minimum threshold (−20 dBm) at the controller/users, so the overall system is still able to detect the FSO signal and extract the original data without detection. The feasibility of FSO communications technology from the atmospheric context of Bangladesh has been analyzed for smart village energy autonomous systems in [104].

## 4. Challenges of Smart Grid Communication

In this section we will discuss future trends of SG communications and applications, and a comprehensive review of these challenges.

### 4.1. Reliable Transmission

Reliable transmission of information with high QoS is one of the most prioritized requirements for SG communications. It will greatly improve the system robustness and reliability by harnessing the modern and secure communication protocols, the communication technologies, faster and more robust control devices and Intelligent Electronic Devices (IEDs) for the entire grid from substation and feeder to customer resources [105]. As the use of communication systems in other scenarios, there are many challenges to achieve robust transmission because of limited bandwidth, limited power, or adverse transmission environment (interference, high path loss, etc.) [106–110]. As discussed in the previous sections, both wireless and wired communication technique consists important parts of the SG communication with its own advantages and disadvantages. In many cases, a hybrid communication technology mixed with wired and wireless solutions can be used in order to provide higher level of system reliability, robustness and availability [111].

### 4.2. Security

Cyber security is considered to be one of the biggest challenges to SG deployment as the power grid becomes more and more interconnected. With the number of connected devices increasing, the possibility for cyber attacks against the power grid will increase. Cyber security is essential as every aspect of the SG must be secure [112,113]. Security measures must cover issues involving communication and automation that affects operation of the power system and the utilities managing them. It must address deliberate attacks as well as inadvertent accidents such as user error and equipment failure [13,112].

SGs are vulnerable to cyber-attacks due to the integration of communication paths throughout the grid infrastructure. SGs are still evolving, and considering security in a new SG environment is important, but challenging. Undetected cyber-attacks can lead to critical damage affecting thousands or millions of customers and life threatening infrastructure [114,115]. Securing the data is vital for both end-user and power companies to ensure trust. As more functions and capabilities are implemented to the SG importance of secure and safe communication increase. From distributed energy generation, energy storage, electric vehicles to power station and power grid control systems. Additionally, something possibly as trivial as securing that the reading from the end-user's smart meters are sending correct billing information, or that the utilities companies receive the correct information is essential [116]. As for any other communication systems, security enhancement for SG communication can be achieved at different layer of the protocol by utilizing the techniques from the conventional upper layer cryptography [117–121] to the physical layer security [122–125]. Different communication technologies, wired and wireless, interconnects and are required to operate the grid securely. Different authorities are responsible securing different data and security aspects in Smart Grid/smart metering. For the Norwegian case:

- Norwegian Metrology Service: Measurement accuracy
- Norwegian Directorate for Civil Protection (DSB): Electrical safety
- Norwegian Communications Authority: Communication
- Norwegian Water Resources and Energy directorate: Application, function, and safety of smart meters.

**Table 6.** Overview of wired communication technologies in SG [20,34,57,72,74].

| **Wired Communication Technologies** | | | | | | |
|---|---|---|---|---|---|---|
| **Technology** | **Data Rate** | **Coverage** | **Application** | **Advantages** | **Disadvantages** | **Network Type** |
| Ethernet | Up to 100 Gbps | Up to 100 m | In-home communication, SCADA, backbone commnunication | Good on short distances | Coverage limitations | Premise network, NAN/FAN, WAN |
| Broadband PLC | Up to 300 Mbps | Up to 1500 m | SCADA, backbone communication in power generation domain | Existing infrastructure, standardized, high reliability | Noisy channel environment, Disturbance | NAN/FAN, WAN |
| Narrowband PLC | 10-500 Kbps | Up to 3 km | SCADA, backbone communication in power generation domain | Existing infrastructure, standardized, high reliability | Noisy channel environment, Disturbance | NAN/FAN, WAN |
| HomePlug | 4, 5, 10 Mbps | Up to 200 m | In-home communication, Smart appliances | Low cost, low energy | Coverage limitations, Disturbance | Premise network |
| Fiber optic | Up to 100 Gbps | Up to 100 km | SCADA, backbone communication in power generation domain | High bandwidth, high data rate. not susceptible to electromagnetic interference | Costly | WAN |

**Table 7.** Overview of wireless communication technologies in SG [20,57,81–86,92–94,97].

| **Wireless Communication Technologies** | | | | | | |
|---|---|---|---|---|---|---|
| **Technology** | **Data Rate** | **Coverage** | **Application** | **Advantages** | **Disadvantages** | **Network Type** |
| WiMAX | 75 Mbps | Up to 50 km | In-home communication<br>Smart meter reading | Low cost, low energy | Not widespread, coverage highly reduced if loss in line of sight | NAN/FAN, WAN |
| ZigBee | 20–250 kbps | Up to 100 m | In-home communication, energy monitoring, smart appliances, home automation | Mesh capability, simplicity, mobility, low energy, low cost. | Low data rate, short range, interference | Premise network, NAN/FAN |
| Z-Wave | 9-40 kbps | Up to 30 m | Wireless mesh network | Mesh capability, simplicity, mobility, low energy, low cost. | Low data rate, short range, interference | Premise network |
| Wi-Fi | 2 Mbps–1.7 Gbps | Up to 100 m | In-come communication, smart appliances, home automation, SCADA | Good on short distances. | Security | Premise network, NAN/FAN |
| 3G | Up to 42 Mbps | 70 km | SCADA,<br>Smart meter reading | Already existing network, high security, low cost, large coverage | Network shared with consumers may result in congestion. | NAN/FAN, WAN |
| 4G/LTE | Up to 979 Mbps | Up to 16 km | SCADA,<br>Smart meter reading | Already existing network, high security, low cost, large coverage | Network shared with consumers may result in congestion. | NAN/FAN, WAN |
| LTE-M | 7 Mbps | 11 km | Smart meter reading | Low cost, low energy, scalability, coverage | Lower data rate | NAN/FAN |
| NB-IoT | 159 kbps | | Smart meter reading | Low cost, low energy, scalability, coverage | Lower data rate | NAN/FAN |
| 5G | Up to 20 Gbps | | SCADA, Remote control<br>Smart meter reading | Low energy, Low latency,<br>High data rate, scalability | | NAN/FAN, WAN |
| Satellite | 50 Mbps | | Backup, remote location communication | Good when no other alternative is viable | High cost | WAN |

Section 13 in The personal data act, sets requirements for satisfactory information security [126]. Based on this, the Norwegian Electrotechnical Committee (NEK) emphasizes on the following three aspects in relation to security in SGs: confidentiality, integrity and availability, as well as the following four elements [127].

- Protection against unauthorized access to measurement data on the meter.
- Protection against unauthorized retrieval of measurement data.
- Protection against tampering or alteration of measurement data.
- Ensuring that measurement data is available when needed.

Vulnerabilities and threats may also be categorized as consumer threat, naturally occurring threat, individual and organizational threat, impacts on consumer, impacts on availability, financial impacts, and likelihood of attack [128]. NEK recommends that communication in HAN use synchronous encryption AES-128, since the data has fixed length. The end-user have to request the utility company to open up for HAN, and to receive encryption key [129]. In Norway, the Norwegian Data Protection Authority (DPA) has identified several aspects relating to SG and smart metering privacy. Since the smart meters can be linked to an address and home-owner, behavioral information can be traced back to individual person [130]. Earlier SCADA systems were isolated on a separate computer network, but the development towards connecting all devices to the Internet are making the system vulnerable to cyber-attacks [131,132]. Attacks have been carried out on SCADA networks in the past, some with significant impact to infrastructure and power delivery [133]. Attacks on Smart Grids can occur on all levels, from generation and distribution to home networks, it can be protocol-based attacks, routing attacks, intrusion, malware and denial-of-service attacks (DoS). Successful attacks can lead to grid instability, or in the worst case failure and blackouts [116,128,134]. A reliable SG depends on avoiding attacks, or detecting and establishing mitigation measures. Protection should be used within SG for message authentication, integrity, and encryption. Security must also address loss of communication, unauthorized access to network and devices (eavesdropping), network attacks, DoS, Distributed Denial of Service (DDoS), Man-in-the-middle (MITM), and jamming of radio signals [78]. There have been several attacks on power companies in the last years, where some have led to system failure and blackout. In 2006 a nuclear power plant in Alabama, USA failed due to overload on the control system network. Investigations later identified the source to be manipulated smart meter power readings [134]. In 2013–2014 an attack affected more than 1000 energy companies in 84 countries including Germany, France, Italy, Spain, Poland, and the US [135]. In December 2015, Ukraine experienced a cyber attack on three regional power distribution companies, leaving people in the dark for over six hours. Over two months after the attack, control centers were not fully operational. The attack was distributed via spear-phishing email, targeting IT staff and systems administrators in companies responsible for power distribution. By opening an attachment in an email, malicious firmware were uploaded SCADA-network. The intruders gained access to substation control centers via Virtual Private Networks (VPNs) and was able to send commands to disable Uninterruptible Power Supply (UPS) systems, and open breakers in substations. The blackout affected around 225,000 customers, and manual operations were required to turn the power back on [114,133]. In 2016 Ukrainian power distribution was once again attacked, parts of the city of Kyiv lost power for an hour. The malware enabled control of circuit breakers to the attackers. In 2020, the European Network of Transmission System Operations for Electricity experienced an attack on its office network. The attack did however not infect any of the systems responsible for controlling the power grid [135,136].

**Denial of service attack**

It has been claimed that DoS attacks are one of the greatest concerns for service providers. Smart Grids consists of a number of measurement devices such as smart meters, smart appliances, data aggregators, PMUs, IEDs, RTUs, PLCs, etc. Attacks on SGs can result in loss of data availability, loss of communication control, compromised data integrity, and loss of power [137].

**Use of encryption**

The security of the power grid is depends on authentication, authorization. Encryption of communication flowing between devices in the grid and data centers is crucial to reduce attackers ability to gain access to data or achieve system control. Depending on communication technology, different solutions are preferred, such as Advanced Encryption Standard (AES) and Triple Data Encryption (TDES) [112]. Encryption ensures identification and authorization.

**Authentication and authorization**

Authentication is the process of verifying the identity of a user, application, or device. Authorization in the process of verifying whether the user, application or device has permission or the rights to access the system, or perform an operation. Authentication, authorization, and access control is necessary in SGs due to the vast amounts of connected devices. Different users with different roles and level have access to control systems, sensors communication networks in the Smart Grid. Entities in the SG must be bidirectionally authenticated. Common types of authentication schemes in Smart Grids are device-to-device, device-to-network, and user-to-network [138].

### *4.3. Privacy*

Communication in SGs are often linked to information related to individual customers and their lives. This is why securing authentication, authorization, and confidentiality is so important in a SG environment. It is of greatest importance not to disclose private data to anyone other than consented entities. Private data include consumer identification, address, and energy usage information [47]. Smart meters are expected to provide high accuracy reading of power consumption at defined time intervals to the utilities companies. This data is used for billing purposes and grid management. However, measurement data from smart meter may be used for other purposes. Usage pattern analysis can be useful for power saving, but involves a significant risk. The data holds a great amount of information about individual consumers [55,139]. Non-intrusive Appliance Load Monitoring (NALM) technologies uses extracts detailed information on appliance use based on energy measurements [140]. By analyzing data and usage patterns, it may be possible to predict when people are at home or away from home, or what appliances are in use. This information is could be of interest for the police, tax authorities, insurance companies, etc. [19,141]. NIST have acknowledged that the major benefit of SGs is the ability to receive richer data from smart meters and devices, is also the biggest weakness from a privacy standpoint.

## 5. Conclusions

In this paper, an overview of SG infrastructure, communications technologies, and its requirements, and applications in premises network, neighborhood area network, and wide area network were presented. Cyber security challenges are briefly presented. We are currently in the brief beginning of what will be a major change in how electric power grids and power generation are organized and managed. The changes are likely to be significant, and new possibilities emerge as new technologies are further developed. The amount of data and information exchange are increasing rapidly as new technologies are implemented to the grid. Security concerns must be addressed to ensure a reliable power supply.

**Author Contributions:** Conceptualization, F.E.A. and Y.A.; methodology, F.E.A. and Y.A.; investigation, F.E.A. and Y.A.; data curation, F.E.A. and Y.A.; writing—original draft preparation, F.E.A. and Y.A.; writing—review and editing, F.E.A., Y.A. and M.C.; visualization, F.E.A.; supervision, Y.A. and M.C.; funding acquisition, F.E.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** The work was funded by the Norwegian University of Science and Technology (NTNU).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Zhou, X.; Ma, Y.; Gao, Z.; Wang, H. Summary of smart metering and smart grid communication. In Proceedings of IEEE International Conference on Mechatronics and Automation (ICMA), Takamatsu, Japan, 6–9 August 2017; pp. 300–304.
2. Priya, P.P.S.; Saminadan, V. Performance analysis of WiMAX based smart grid communication traffic priority model. In Proceedings of the International Conference on Communication and Signal Processing, Melmaruvathur, India, 3–5 April 2014; pp. 778–782.
3. Farhangi, H. The path of the smart grid. *IEEE Power Energy Mag.* **2009**, *8*, 18–28. [CrossRef]
4. Dileep, G. A survey on smart grid technologies and applications. *Renew. Energy* **2020**, *146*, 2589–2625. [CrossRef]
5. Norwegian Smart Grid Research Centre. *Norwegian Smart Grid Research Strategy*; Norwegian Smart Grid Research Centre. 2015. Available online: https://smartgrids.no/wp-content/uploads/sites/4/2015/08/Norwegian-Smart_Grid__Research_Strategy_DRAFT_June10_WT_ks_hii.pdf (accessed on 9 November 2021).
6. Elhub. *Årsrapport 2020*; Elhub 2021. Available online: https://elhub.no/documents/2021/06/elhub-arsrapport-2020.pdf/ (accessed on 9 November 2021).
7. European Commission Joint Research Centre Smart Electricity and Interoperability. Smart Metering Deployment in the European Union. Available online: https://ses.jrc.ec.europa.eu/smart-metering-deployment-european-union (accessed on 20 October 2020).
8. Global Smart Grid Federation. *Smart Meter Security Survey*; Global Smart Grid Federation: Washington, DC, USA, 2016.
9. International Energy Agency. *Technology Roadmap*. International Energy Agency. Available online: https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf (accessed on 18 October 2020).
10. Ghalib, M.; Ahmed, A.; Al-Shiab, I.; Bouida, Z.; Ibnkahla, M. Implementation of a smart grid communication system compliant with IEEE 2030.5. In Proceedings of the 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
11. International Electrotechnical Commission. *IEC Smart Grid Standardization Roadmap*; SMB Smart Grid Strategic Group (SG3): Geneva, Switzerland, 2010.
12. National Institute of Standards and Technology. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*; Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2010.
13. National Institute of Standards and Technology. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*; Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014.
14. National Institute of Standards and Technology. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0*; Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021.
15. DKE, German Commission for Electrical, Information Technologies of DIN and VDE. The German Roadmap E-Energy/Smart Grid 2.0. Available online: https://www.dke.de/resource/blob/778304/96de7a637009007d65182df8c4d1a9aa/the-german-roadmap-e-energy-smart-grids-version-2-0-data.pdf (accessed on 15 September 2019).
16. ITU Telecommunication Standardization Bureau Policy & Technology Watch Division. Activities in Smart Grid Standardization Repository (Version 2.0, April 2011). Available online: https://www.itu.int/en/ITU-T/focusgroups/smart/Documents/smartgrid_repository-V2.pdf (accessed on 4 September 2019).
17. Chren, S.; Rossi, B.; Pitner, T. Smart grids deployments within EU projects: The role of smart meters. In Proceedings of the 2016 Smart Cities Symposium Prague (SCSP), Prague, Czech Republic, 26–27 May 2016; pp. 1–5.
18. Gözde, H.; Taplamacıoğlu, M.C.; Arı, M.; Shalaf, H. 4G/LTE technology for smart grid communication infrastructure. In Proceedings of the International Istanbul Smart Grid Congress and Fair (ICSG), Istanbul, Turkey, 29–30 April 2015; pp. 1–4.
19. Goel, S.; Hong, Y.; Papakonstantinou, V.; Kloza, D. *Smart Grid Security*, 1st ed.; Springer: London, UK, 2015.
20. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput. Netw.* **2014**, *67*, 74–88. [CrossRef]
21. Qarabsh, N.A.; Sabry, S.S.; Qarabash, H.A. Smart grid in the context of industry 4.0: An overview of communications technologies and challenges. *Indones. J. Electr. Eng. Comput. Sci.* **2020**, *18*, 656–665. [CrossRef]
22. National Institute of Standards and Technology. *Update of the NIST Smart Grid Conceptual Model (Discussion DRAFT)*; Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
23. Hossain, E.; Han, Z.; Poor, H.V. *Smart Grid Communications and Networking*; Cambridge University Press: Cambridge, UK, 2012.
24. Ma, R.; Chen, H.H.; Huang, Y.R.; Meng, W. Smart grid communication: Its challenges and opportunities. *IEEE Trans. Smart Grid* **2013**, *4*, 36–46. [CrossRef]

25. Samad, T.; Annaswamy, A.M. Controls for smart grids: Architectures and applications. *Proc. IEEE* **2017**, *105*, 2244–2261. [CrossRef]
26. Souri, H.; Dhraief, A.; Tlili, S.; Drira, K.; Belghith, A. Smart metering privacy-preserving techniques in a nutshell. *Procedia Comput. Sci.* **2014**, *32*, 1087–1094. [CrossRef]
27. European Committee for Electrotechnical Standardization. CEN-CENELEC-ETSI Smart Grid Coordination Group—Framework Document, 2012. Available online: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf (accessed on 1 September 2019).
28. Smart Grids Austria. *Smart Grids Austria Technology Roadmap*; Media Proprietor, Technology Platform Smart Grids: Vienna, Austria, 2015
29. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [CrossRef]
30. Kabalci, E.; Kabalci, Y. Introduction to smart grid architecture. In *Smart Grids and Their Communication Systems*; Springer: Berlin, Germany, 2019; pp. 3–45.
31. Bouwmeester, J.; van der Linden, S.; Povalac, A.; Gill, E. Towards an innovative electrical interface standard for PocketQubes and CubeSats. *Adv. Space Res.* **2018**, *62*, 3423–3437. [CrossRef]
32. Fines, S. AMS og HAN-grensesnittet. In *NEKs Elsikkerhetskonferanse 2017*; Norsk Elektroteknisk Komite: Oslo, Norway, 2017. Available online: https://www.nek.no/wp-content/uploads/2017/11/4-22-11-1110-1135-Steinar-Fines-AMS-HAN-Grensesnittet.pdf (accessed on 10 September 2019).
33. Syed, D.; Zainab, A.; Ghrayeb, A.; Refaat, S.S.; Abu-Rub, H.; Bouhali, O. Smart grid big data analytics: Survey of technologies, techniques, and applications. *IEEE Access* **2020**, *9*, 59564–59585. [CrossRef]
34. Faheem, M.; Shah, S.B.H.; Butt, R.A.; Raza, B.; Anwar, M.; Ashraf, M.W.; Ngadi, M.A.; Gungor, V.C. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Comput. Sci. Rev.* **2018**, *30*, 1–30. [CrossRef]
35. Salinas, S.; Li, M.; Li, P.; Fu, Y. Dynamic energy management for the smart grid with distributed energy resources. *IEEE Trans. Smart Grid* **2013**, *4*, 2139–2151. [CrossRef]
36. Tushar, W.; Chai, B.; Yuen, C.; Smith, D.B.; Wood, K.L.; Yang, Z.; Poor, H.V. Three-party energy management with distributed energy resources in smart grid. *IEEE Trans. Ind. Electron.* **2014**, *62*, 2487–2498. [CrossRef]
37. Hui, H.; Ding, Y.; Shi, Q.; Li, F.; Song, Y.; Yan, J. 5G network-based Internet of Things for demand response in smart grid: A survey on application potential. *Appl. Energy* **2020**, *257*, 113972. [CrossRef]
38. Shahinzadeh, H.; Mirhedayati, A.S.; Shaneh, M.; Nafisi, H.; Gharehpetian, G.B.; Moradi, J. Role of Joint 5G-IoT Framework for Smart Grid Interoperability Enhancement. In Proceedings of the 2020 15th International Conference on Protection and Automation of Power Systems (IPAPS), Shiraz, Iran, 30–31 December 2020; pp. 12–18.
39. Zhang, J.; Hasandka, A.; Alam, S.S.; Elgindy, T.; Florita, A.R.; Hodge, B.M. Analysis of hybrid smart grid communication network designs for distributed energy resources coordination. In Proceedings of the 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–21 February 2019; pp. 1–5.
40. Ahmadzadeh, S.; Parr, G.; Zhao, W. A Review on Communication Aspects of Demand Response Management for Future 5G IoT-Based Smart Grids. *IEEE Access* **2021**, in press. [CrossRef]
41. Lopes, J.A.P.; Madureira, A.G.; Matos, M.; Bessa, R.J.; Monteiro, V.; Afonso, J.L.; Santos, S.F.; Catalão, J.P.; Antunes, C.H.; Magalhães, P. The future of power systems: Challenges, trends, and upcoming paradigms. *Wiley Interdiscip. Rev. Energy Environ.* **2020**, *9*, e368. [CrossRef]
42. Logenthiran, T.; Srinivasan, D. Intelligent management of distributed storage elements in a smart grid. In Proceedings of the IEEE Ninth International Conference on Power Electronics and Drive Systems, Singapore, 5–8 December 2011; pp. 855–860.
43. Liu, C.; Chau, K.; Wu, D.; Gao, S. Opportunities and challenges of vehicle-to-home, vehicle-to-vehicle, and vehicle-to-grid technologies. *Proc. IEEE* **2013**, *101*, 2409–2427. [CrossRef]
44. Bach Andersen, P.; Hashemi, S.; Sousa, T.; Meier Soerensen, T.; Noel, L.; Christensen, B. The Parker Project: Cross-Brand Service Testing Using V2G. *World Electr. Veh. J.* **2019**, *10*, 66. [CrossRef]
45. Balakumar, P.; Sathiya, S. Demand side management in smart grid using load shifting technique. In Proceedings of the IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), Karur, India, 27–28 April 2017; pp. 1–6.
46. Mohagheghi, S.; Yang, F.; Falahati, B. Impact of demand response on distribution system reliability. In Proceedings of the IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24-28 July 2011; pp. 1–7.
47. Tsado, Y.; Lund, D.; Gamage, K.A. Resilient communication for smart grid ubiquitous sensor network: State of the art and prospects for next generation. *Comput. Commun.* **2015**, *71*, 34–49. [CrossRef]
48. Budka, K.C.; Deshpande, J.G.; Thottan, M. *Communication Networks for Smart Grids*; Springer: Berlin, Germany, 2016.
49. Balijepalli, V.M.; Pradhan, V.; Khaparde, S.; Shereef, R. Review of demand response under smart grid paradigm. In Proceedings of the Innovative Smart Grid Technologies Conference (ISGT), Kollam, India, 1–3 December 2011; pp. 236–243.
50. Jeon, Y-H. QoS requirements for the smart grid communications system. *Int. J. Comput. Sci. Netw. Secur.* **2011**, *11*, 86–94.

51. Ustun, T.S.; Hadbah, A.; Kalam, A. Interoperability and interchangeability considerations in microgrids employing IEC61850 standard. In Proceedings of the 2013 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 28–30 August 2013; pp. 1–5.
52. Aftab, M.A.; Hussain, S.S.; Ali, I.; Ustun, T.S. IEC 61850 and XMPP communication based energy management in microgrids considering electric vehicles. *IEEE Access* **2018**, *6*, 35657–35668. [CrossRef]
53. Kumari, N.; Chernogorov, F.; Ashraf, I.; Torsner, J.; Kronander, J.; Wikström, G.; Sahoo, S. Enabling process bus communication for digital substations using 5G wireless system. In Proceedings of the 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Istanbul, Turkey, 8–11 September 2019; pp. 1–7.
54. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [CrossRef]
55. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 21–38. [CrossRef]
56. Wang, W.; Xu, Y.; Khanna, M. A survey on the communication architectures in smart grid. *Comput. Netw.* **2011**, *55*, 3604–3629. [CrossRef]
57. Saputro, N.; Akkaya, K.; Uludag, S. A survey of routing protocols for smart grid communications. *Comput. Netw.* **2012**, *56*, 2742–2771. [CrossRef]
58. Meng, W.; Ma, R.; Chen, H.H. Smart grid neighborhood area networks: A survey. *IEEE Netw.* **2014**, *28*, 24–32. [CrossRef]
59. Mohassel, R.R.; Fung, A.; Mohammadi, F.; Raahemifar, K. A survey on advanced metering infrastructure. *Int. J. Electr. Power Energy Syst.* **2014**, *63*, 473–484. [CrossRef]
60. Aravind, E.; Vasudevan, S.K. Smart meter based on real time pricing. *Procedia Technol.* **2015**, *21*, 120–124.
61. Parikh, P.P.; Kanabar, M.G.; Sidhu, T.S. Opportunities and challenges of wireless communication technologies for smart grid applications. In Proceedings of the IEEE PES General Meeting, Minneapolis, MN, USA, 25–29 July 2010; pp. 1–7.
62. Lee, J.J.; Kim, Y.H.; Bae, J.M.; Seo, J.K.; Nam, D.H.; Kim, J.Y.; In, D.S. AMR field trial on underground power distribution line using BPLC. In Proceedings of the IEEE International Symposium on Power Line Communications and Its Applications, Udine, Italy, 3–6 April 2011; pp. 204–208.
63. Emmanuel, M.; Rayudu, R. Communication technologies for smart grid applications: A survey. *J. Netw. Comput. Appl.* **2016**, *74*, 133–148. [CrossRef]
64. Ai, Y.; Cheffena, M. Capacity analysis of PLC over Rayleigh fading channels with colored Nakagami-*m* additive noise. In Proceedings of the IEEE Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18–21 September 2016; pp. 1–5.
65. Mathur, A.; Ai, Y.; Cheffena, M.; Bhatnagar, M.R. Performance of Hybrid ARQ over Power Line Communications Channels. In Proceedings of the IEEE Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–6.
66. Pinomaa, A.; Ahola, J.; Kosonen, A.; Nuutinen, P. Noise analysis of a power-line communication channel in an LVDC smart grid concept. In Proceedings of the IEEE International Symposium on Power Line Communications and Its Applications, Johannesburg, South Africa, 24–27 March 2013; pp. 41–46.
67. Ai, Y.; Bhatnagar, M.R.; Cheffena, M.; Mathur, A.; Sedakov, A. Game-theoretical analysis of PLC system performance in the presence of jamming attacks. In Proceedings of the International Conference on Decision and Game Theory for Security, Vienna, Austria, 23–25 October 2017; pp. 74–90.
68. Ai, Y.; Ohtsuki, T.; Cheffena, M. Performance analysis of PLC over fading channels with colored Nakagami-*m* background noise. In Proceedings of the IEEE Vehicular Technology Conference (VTC Spring), Sydney, Australia, 4–7 June 2017; pp. 1–6.
69. Ai, Y.; Kong, L.; Cheffena, M.; Chatzinotas, S.; Ottersten, B. On Performance Characterization of Cascaded Multiwire-PLC/MIMO-RF Communication System. *arXiv* **2020**, arXiv:2010.04099.
70. Song, J.; Ding, W.; Yang, F.; Yang, H.; Yu, B.; Zhang, H. An indoor broadband broadcasting system based on PLC and VLC. *IEEE Trans. Broadcast.* **2015**, *61*, 299–308. [CrossRef]
71. Mathur, A.; Bhatnagar, M.R.; Ai, Y.; Cheffena, M. Performance analysis of a dual-hop wireless-power line mixed cooperative system. *IEEE Access* **2018**, *6*, 34380–34392. [CrossRef]
72. Hazen, M.E. The technology behind homeplug av powerline communications. *Computer* **2008**, *41*, 90–92. [CrossRef]
73. Pinomaa, A.; Ahola, J.; Kosonen, A.; Nuutinen, P. HomePlug green PHY for the LVDC PLC concept: Applicability study. In Proceedings of the IEEE International Symposium on Power Line Communications and Its Applications (ISPLC), Austin, TX, USA, 29 March–1 April 2015; pp. 205–210.
74. Bian, D.; Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Analysis of communication schemes for advanced metering infrastructure (AMI). In Proceedings of the IEEE PES General Meeting | Conference & Exposition, National Harbor, MD, USA, 27–31 July 2014; pp. 1–5.
75. Karagiannis, G.; Pham, G.T.; Nguyen, A.D.; Heijenk, G.J.; Haverkort, B.R.; Campfens, F. Performance of LTE for smart grid communications. In Proceedings of the International Conference on Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance, Bamberg, Germany, 17–19 March 2014; pp. 225–239.
76. Surgiewicz, R.; Strom, N.; Ahmed, A.; Ai, Y. *LTE Uplink Transmission Scheme*; Chalmers University of Technology: Gothenburg, Sweden, 2014.

77. Cheng, P.; Wang, L.; Zhen, B.; Wang, S. Feasibility study of applying LTE to Smart Grid. In Proceedings of the IEEE International Workshop on Smart Grid Modeling and Simulation (SGMS), Brussels, Belgium, 17 October 2011; pp. 108–113.
78. De Dutta, S.; Prasad, R. Security for smart grid in 5G and beyond networks. *Wirel. Pers. Commun.* **2019**, *106*, 261–273. [CrossRef]
79. El-Dessouki, I.; Saeed, N. Smart Grid Integration into Smart Cities. In Proceedings of the 2021 IEEE International Smart Cities Conference (ISC2), Manchester, UK, 7–10 September 2021; pp. 1–4.
80. Chen, J.; Zhu, H.; Chen, L.; Li, Q.; Bian, B.; Xia, X. 5G Enabling Digital Transformation of Smart Grid: A Review of Pilot Projects and Prospect. In Proceedings of the 2021 IEEE/CIC International Conference on Communications in China (ICCC Workshops), Xiamen, China, 28–30 July 2021; pp. 353–357.
81. Dragičević, T.; Siano, P.; Prabaharan, S. Future generation 5G wireless networks for smart grid: A comprehensive review. *Energies* **2019**, *12*, 2140.
82. Mao, R.; Julka, V. WiMAX for advanced metering infrastructure. In Proceedings of the International Conference on Green and Ubiquitous Technology, Bandung, Indonesia, 7–8 July 2012; pp. 15–19.
83. Usman, A.; Shami, S.H. Evolution of communication technologies for smart grid applications. *Renew. Sustain. Energy Rev.* **2013**, *19*, 191–199. [CrossRef]
84. Rengaraju, P.; Lung, C.H.; Srinivasan, A. Communication requirements and analysis of distribution networks using WiMAX technology for smart grids. In Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC), Limassol, Cyprus, 27–31 August 2012; pp. 666–670.
85. Parvez, I.; Sundararajan, A.; Sarwat, A.I. Frequency band for HAN and NAN communication in Smart Grid. In Proceedings of the IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG), Orlando, FL, USA, 9–12 December 2014; pp. 1–5.
86. Mahmood, A.; Javaid, N.; Razzaq, S. A review of wireless communications for smart grid. *Renew. Sustain. Energy Rev.* **2015**, *41*, 248–260. [CrossRef]
87. Zafar, R.; Mahmood, A.; Razzaq, S.; Ali, W.; Naeem, U.; Shehzad, K. Prosumer based energy management and sharing in smart grid. *Renew. Sustain. Energy Rev.* **2018**, *82*, 1675–1684. [CrossRef]
88. Burunkaya, M.; Pars, T. A smart meter design and implementation using ZigBee based wireless sensor network in smart grid. In Proceedings of the International Conference on Electrical and Electronic Engineering (ICEEE), Ankara, Turkey, 8–10 April 2017; pp. 158–162.
89. Ai, Y.; Cheffena, M.; Li, Q. Radio frequency measurements and capacity analysis for industrial indoor environments. In Proceedings of the European Conference on Antennas and Propagation (EuCAP), Lisbon, Portugal, 13–17 April 2015; pp. 1–5.
90. Cheffena, M. Industrial Wireless Communications over the Millimeter Wave Spectrum: Opportunities and Challenges. *IEEE Commun. Mag.* **2016**, *54*, 66–72. [CrossRef]
91. Ai, Y.; Cheffena, M.; Li, Q. Power delay profile analysis and modeling of industrial indoor channels. In Proceedings of the European Conference on Antennas and Propagation (EuCAP), Lisbon, Portugal, 13–17 April 2015; pp. 1–5.
92. Bekara, C. Security Issues and Challenges for the IoT-Based Smart Grid. *Procedia Comput. Sci.* **2014**, *34*, 532–537. [CrossRef]
93. Samuel, S.S.I. A review of connectivity challenges in IoT-smart home. In Proceedings of the MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 15–16 March 2016; pp. 1–4.
94. Granelli, F.; Domeniconi, D.; Da Fonseca, N.L.; Tsetsgee, B. On the Usage of WiFi and LTE for the Smart Grid. In Proceedings of the International Conference on Ubi-Media Computing and Workshops, Ulaanbaatar, Mongolia, 12–14 July 2014; pp. 1–5.
95. Li, L.; Xiaoguang, H.; Ke, C.; Ketai, H. The applications of wifi-based wireless sensor network in internet of things and smart grid. In Proceedings of the IEEE Conference on Industrial Electronics and Applications, Beijing, China, 21–23 June 2011; pp. 789–793.
96. Meloni, A.; Atzori, L. The role of satellite communications in the smart grid. *IEEE Wirel. Commun.* **2017**, *24*, 50–56. [CrossRef]
97. De Sanctis, M.; Cianca, E.; Araniti, G.; Bisio, I.; Prasad, R. Satellite communications supporting internet of remote things. *IEEE Internet Things J.* **2015**, *3*, 113–123. [CrossRef]
98. Abrahamsen, F.E.; Ai, Y.; Wold, K.; Mohamed, M. Free-Space Optical Communication: From Space to Ground and Ocean. *IEEE Potentials* **2021**, in press. [CrossRef]
99. Ai, Y.; Mathur, A.; Cheffena, M.; Bhatnagar, M.R.; Lei, H. Physical layer security of hybrid satellite-FSO cooperative systems. *IEEE Photonics J.* **2019**, *11*, 1–14. [CrossRef]
100. Verma, G.D.; Mathur, A.; Ai, Y.; Cheffena, M. Secrecy performance of FSO communication systems with nonzero boresight pointing errors. *IET Commun.* **2021**, *15*, 155–162. [CrossRef]
101. Ai, Y.; Mathur, A.; Lei, H.; Cheffena, M.; Ansari, I.S. Secrecy enhancement of RF backhaul system with parallel FSO communication link. *Opt. Commun.* **2020**, *475*, 126193. [CrossRef]
102. Ai, Y.; Mathur, A.; Verma, G.D.; Kong, L.; Cheffena, M. Comprehensive Physical Layer Security Analysis of FSO Communications over Mlaga Channels. *IEEE Photonics J.* **2020**, *6*, 1–7. [CrossRef]
103. Sivakumar, P.; Nagaraju, R.; Samanta, D.; Sivaram, M.; Hindia, M.N.; Amiri, I.S. A novel free space communication system using nonlinear InGaAsP microsystem resonators for enabling power-control toward smart cities. *Wirel. Netw.* **2020**, *26*, 2317–2328. [CrossRef]
104. Haider, M.F.; Siddique, A.R.; Alam, S. An approach to implement frees space optical (FSO) technology for smart village energy autonomous systems. *Far East J. Electron. Commun.* **2018**, *18*, 439–456. [CrossRef]

105. Moslehi, K.; Kumar, R. Smart grid—A reliability perspective. In Proceedings of the Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 19–21 January 2010; pp. 1–8.
106. Ai, Y.; Cheffena, M. A comparative study of wireless channel propagation characteristics in industrial and office environments. In Proceedings of the International Symposium on Antennas and Propagation (ISAP), Hobart, Australia, 9–12 November 2015.
107. Güzelgöz, S.; Arslan, H.; Islam, A.; Domijan, A. A review of wireless and PLC propagation channel characteristics for smart grid environments. *J. Electr. Comput. Eng.* **2011**, *2011*, 154040. [CrossRef]
108. Ai, Y.; Andersen, J.B.; Cheffena, M. Path-loss prediction for an industrial indoor environment based on room electromagnetics. *IEEE Trans. Antennas Propag.* **2017**, *65*, 3664–3674. [CrossRef]
109. Al-Samman, A.M.; Mohamed, M.; Ai, Y.; Cheffena, M.; Azmi, M.H.; Rahman, T.A. Rain attenuation measurements and analysis at 73 GHz E-band link in tropical region. *IEEE Commun. Lett.* **2020**, *24*, 1368–1372. [CrossRef]
110. Ai, Y.; Cheffena, M. On multi-hop decode-and-forward cooperative relaying for industrial wireless sensor networks. *Sensors* **2017**, *17*, 695. [CrossRef] [PubMed]
111. Zhang, J.; Hasandka, A.; Wei, J.; Alam, S.; Elgindy, T.; Florita, A.R.; Hodge, B.M. Hybrid communication architectures for distributed smart grid applications. *Energies* **2018**, *11*, 871. [CrossRef]
112. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010. [CrossRef]
113. Ghanem, K.; Asif, R.; Ugwuanyi, S.; Irvine, J. Bandwidth and Security Requirements for Smart Grid. In Proceedings of the 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), The Hague, The Netherlands, 26–28 October 2020; pp. 36–40.
114. Saxena, N.; Xiong, L.; Chukwuka, V.; Grijalva, S. Impact evaluation of malicious control commands in cyber-physical smart grids. *IEEE Trans. Sustain. Comput.* **2018**, *6*, 208–220. [CrossRef]
115. Yang, Q.; Barria, J.A.; Green, T.C. Communication infrastructures for distributed control of power distribution networks. *IEEE Trans. Ind. Inform.* **2011**, *7*, 316–327. [CrossRef]
116. Sgouras, K.I.; Birda, A.D.; Labridis, D.P. Cyber attack impact on critical smart grid infrastructures. In Proceedings of the Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 19–22 February 2014; pp. 1–5.
117. Iyer, S. Cyber security for smart grid, cryptography, and privacy. *Int. J. Digit. Multimed. Broadcast.* **2011**, *2011*. [CrossRef]
118. He, D.; Wang, H.; Khan, M.K.; Wang, L. Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. *IET Commun.* **2016**, *10*, 1795–1802. [CrossRef]
119. Gope, P.; Sikdar, B. Privacy-aware authenticated key agreement scheme for secure smart grid communication. *IEEE Trans. Smart Grid* **2018**, *10*, 3953–3962. [CrossRef]
120. Sharma, M.; Agarwal, A. Survey on authentication and encryption techniques for smart grid communication. In Proceedings of the India International Conference on Power Electronics (IICPE), Patiala, India, 17–19 November 2016; pp. 1–5.
121. Nicanfar, H.; Leung, V.C. Password-authenticated cluster-based group key agreement for smart grid communication. *Secur. Commun. Netw.* **2014**, *7*, 221–233. [CrossRef]
122. Lee, E.K.; Gerla, M.; Oh, S.Y. Physical layer security in wireless smart grid. *IEEE Commun. Mag.* **2012**, *50*, 46–52. [CrossRef]
123. Ai, Y.; Cheffena, M.; Ohtsuki, T.; Zhuang, H. Secrecy performance analysis of wireless sensor networks. *IEEE Sens. Lett.* **2019**, *3*, 1–4. [CrossRef]
124. Islam, S.N.; Baig, Z.; Zeadally, S. Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6522–6530. [CrossRef]
125. Ai, Y.; Kong, L.; Cheffena, M. Secrecy outage analysis of double shadowed Rician channels. *Electron. Lett.* **2019**, *55*, 765–767. [CrossRef]
126. Norwegian Parliament. Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act). Available online: https://app.uio.no/ub/ujur/oversatte-lover/data/lov-20000414-031-eng.pdf (accessed on 2 September 2019).
127. Aanensen, L.T.; Fines, S.; Ek, R. *AMS + HAN Om å gjøre sanntid måledata tilgjengelig for forbruker*; Report; Norwegian Electrotechnical Committee: Lilleaker, Norway, 2015.
128. Tan, S.; De, D.; Song, W.Z.; Yang, J.; Das, S.K. Survey of security advances in smart grid: A data driven approach. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 397–422. [CrossRef]
129. Norwegian Electrotechnical Committee. *Vedlegg 1 – HAN Personvern – et tillegg til utredningen «AMS + HAN - om å gjøre sanntids måledata tilgjengelig for forbruker»*; Report; Norwegian Electrotechnical Committee: Lilleaker, Norway, 2018
130. Datatilsynet. Automatisk strømmåling. Available online: https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/strommaling/ (accessed on 22 October 2020).
131. Kumar, S.; Gaur, N.; Kumar, A. Developing a Secure Cyber Ecosystem for SCADA Architecture. In Proceedings of the International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 15–16 February 2018; pp. 559–562.
132. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State-of-the-art. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 45–56. [CrossRef]
133. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Trans. Power Syst.* **2016**, *32*, 3317–3318. [CrossRef]

134. Kim, M. A survey on guaranteeing availability in smart grid communications. In Proceedings of the International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South), 19–22 February 2012; pp. 314–317.
135. Kshetri, N.; Voas, J. Hacking power grids: A current problem. *Computer* **2017**, *50*, 91–95. [CrossRef]
136. Fingrid Oyj. *ENTSO-E: Cyber Intrusion on Its Office Network*. Available online: https://www.fingrid.fi/en/pages/news/news/2020/entso-e-cyber-intrusion-on-its-e-office-network/ (accessed on 9 November 2021).
137. Huseinović, A.; Mrdović, S.; Bicakci, K.; Uludag, S. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. *IEEE Access* **2020**, *8*, 177447–177470. [CrossRef]
138. Saxena, N.; Choi, B.J. State of the art authentication, access control, and secure integration in smart grid. *Energies* **2015**, *8*, 11883–11915. [CrossRef]
139. Quinn, E.L. Privacy and the new energy infrastructure. *Soc. Sci. Res. Netw. (SSRN)* **2009**. [CrossRef]
140. Hart, G.W. Nonintrusive appliance load monitoring. *Proc. IEEE* **1992**, *80*, 1870–1891. [CrossRef]
141. Prudenzi, A. A neuron nets based procedure for identifying domestic appliances pattern-of-use from energy recordings at meter panel. In Proceedings of the IEEE Conference on Power Engineering Society Winter Meeting, New York, NY, USA, 27–31 January 2002; Volume 2, pp. 941–946.